VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KRYPTOMĚNY JAKO PLATEBNÍ PROSTŘEDEK V NELEGÁLNÍM OBCHODU

Autor práce: Tadeáš Bělohlávek

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Milan Kocík, MBA

Katedra: Katedra právních oborů a bezpečnostních studií

2024

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Tadeáš Bělohlávek

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaňá
Místo studia: České Budějovice

Název bakalářské práce: Kryptoměny jako platební prostředek v nelegálním obchodu

Název bakalářské práce v anglickém jazyce: Cryptocurrencies as a Payment Method in Illegal Trade

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
JUDr. Milan Kocík MBA
Datum zadání bakalářské práce (měsíc, rok):
Duben 2023
Cíl bakalářské práce:
Hlavním cílem práce je analyzovat využití kryptoměn jako platebního prostředku v nelegálním obchodě a zhodnotit možnosti na jejich právní regulaci. Dílčím cílem práce bude vyhodnotit a definovat kriminologická specifika tohoto platebního prostředku.

Student: Tadeáš Bělohlávek	1.5.2023 *datum*	*podpis*
Vedoucí práce: JUDr. Milan Kocík, MBA	2.5.2023 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	23.5.2023 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	23.5.2023 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	23.5.2023 *datum*	*podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce JUDr. Milanu Kocíkovi, MBA za cenné rady, připomínky a metodické vedení práce. Dále bych rád poděkoval panu nadpraporčíkovi Bc. et BC. Eriku Navrátilovi, který mi poskytl důležité informace k této práci.

ABSTRAKT

BĚLOHLÁVEK, T. *Kryptoměny jako platební prostředek v nelegální obchodu: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2024, 71 s. Vedoucí bakalářské práce: JUDr. Milan Kocík. MBA

Klíčová slova: Kryptoměna, anonymita, kybernetická kriminalita

Bakalářská práce se zabývá kryptoměnou jako platební prostředek při nelegálním obchodu čili autor vypracuje analýzu, jakých protiprávních jednáních se pachatelé dopouštějí s využitím kryptoměn. V teoretické části bude popsán pojem kryptoměna včetně její historie, dále autor definuje kyberprostor, kybernetickou kriminalitu a kybernetickou bezpečnost pomocí odborné rešerše literárních a jiných odborných zdrojů. V praktické části autor zpracuje SWOT matici a povede strukturovaný rozhovor se specialistou ve zkoumané oblasti.

ABSTRACT

BĚLOHLÁVEK, T. *Cryptocurrencies as a Payment Payment in Illegal Trade: Bachelor Thesis.* České Budějovice: University of European and Regional Studies, 2024, 71 p. Bachelor Thesis Supervisor: JUDr. Milan Kocík. MBA

Keywords: Cryptocurrency, anonymity, cybercrime

The bachelor thesis explores cryptocurrencies as a means of payment in illegal trade, analyzing the unlawful activities perpetrators engage in using cryptocurrencies. In the theoretical part, the concept of cryptocurrency, including its history, will be described, and the author will define cyberspace, cybercrime, and cybersecurity through expert research of literary and other professional sources. In the practical part, the author will conduct a SWOT analysis and conduct a structured interview with an expert in the field under investigation.

Obsah

Úvod

Rozvoj kryptoměn, jako je Bitcoin, Ethereum nebo Ripple, způsobil revoluci v oblasti finančních transakcí a digitálního obchodu. Tyto decentralizované digitální měny umožňují uživatelům provádět anonymní a rychlé transakce přes internet bez účasti tradičních bankovních institucí. Nicméně, tento vzestup kryptoměn nese také svůj stín, protože se staly oblíbeným nástrojem pro nelegální aktivity a ilegální obchod.

Tato bakalářská práce se zabývá analýzou role, kterou hrají kryptoměny jako platební prostředek v rámci nelegálního obchodu. Autor zkoumá, jaké jsou hlavní faktory, které přispívají k popularitě kryptoměn mezi různými kriminálními skupinami a jednotlivci zapojenými do nelegálních aktivit. Dále se zaměřuje na technické aspekty použití kryptoměn v nelegálním obchodě, včetně anonymních platebních systémů, tzv. mixérů, a dalších nástrojů, které umožňují skrýt původ finančních prostředků.

Důležitou součástí jsou zhodnocena rizika, která souvisejí s používáním kryptoměn v rámci nelegálního obchodu, včetně otázek týkajících se bezpečnosti, regulace a potenciálního zneužívání těchto digitálních platforem pro praní špinavých peněz a financování terorismu.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce je analyzovat využití kryptoměn jako platebního prostředku v nelegálním obchodě a zhodnotit možnosti na jejich právní regulaci. Dílčím cílem je vyhodnotit a definovat kriminologická specifika tohoto platebního prostředku.

Pro zpracování této práce byly použity následující metody sběru dat:

- Rešerše a analýza odborné literatury a jiných zdrojů
- SWOT matice
- Strukturovaný rozhovor

V teoretické části práce je popsán pojem kryptoměna s ohledem na její historii, klíčové pojmy související a trojici předních tokenů. Dále autor vymezuje prostor, ve kterém jsou kryptoměny získávány, provozovány a používány čili kyberprostor s ohledem na historii a strukturu internetu. Po vysvětlení předešlých pojmů následuje vymezení kyberkriminality a kybernetické bezpečnosti.

V praktické části autor vypracoval SWOT matici, ve které popsal silné stránky, slabé stránky, příležitosti a hrozby kryptoměn s ohledem na možnost využívání v kriminálním prostředí a následně provedl strukturovaný rozhovor s panem nadpraporčíkem Bc. et BC. Erikem Navrátilem z řad Policie ČR. V závěru byla zjištěná data použita k naplnění cílů bakalářské práce.

2 Kryptoměny

Kryptoměny jsou digitální měny. Nejznámější kryptoměnou je Bitcoin. Nicméně existuje mnoho dalších kryptoměn, včetně Ethereum, Ripple a mnoha dalších. Vzhledem k jejich vlastnostem se kryptoměny staly významným fenoménem v oblasti financí a technologií. Avšak jejich volatilita, regulace a bezpečnostní otázky stále vyvolávají diskuse a zkoumání ze strany odborníků i veřejnosti.[1]

2.1 Definice

Existuje mnoho způsobů, jak definovat kryptoměnu, ale veřejně dostupné definice často trpí nedostatečnostmi a někdy se vzájemně liší, což komplikuje výběr správné definice. Ta by měla zahrnovat kritéria pro rozlišení mezi legitimními kryptoměnami a těmi, které jsou podvodné. Podle Lánského lze kryptoměnu popsat jako systém, který splňuje následující podmínky:

- *,,Systém funguje bez potřeby centrální autority a dosahuje distribuovaným způsobem shody o svém stavu.*
- *Uchovává přehled o jednotkách dané kryptoměny a jejího vlastnictví.*
- *Vlastnictví jednotek kryptoměny se prokazuje pouze pomocí kryptografických prostředků.*
- *Systém definuje podmínky pro vznik nových jednotek kryptoměny, včetně okolností vzniku a procesu určení vlastnictví nových jednotek.*
- *Umožňuje provádění transakcí, které vedou ke změně vlastnictví jednotek kryptoměny, a povolení k provedení transakce vydává pouze entita, která dokáže aktuální vlastnictví zmíněných jednotek.*
- *Pokud jsou zadány současně dva rozdílné pokyny ke změně vlastnictví stejných jednotek kryptoměny, systém provede nejvýše jeden z nich‘‘.*[2]

[1] *Fenomén jménem kryptoměny – proč jsou tak populární?* [online] 30.01.2022. Měšec. [cit. 2024-03-11] Dostupné z WWW: https://www.mesec.cz/pr-clanky/fenomen-jmenem-kryptomeny-proc-jsou-tak-popularni/

[2] LÁNSKÝ, J. *Kryptoměny.* Praha: C.H. Beck, 2018. 2 s. ISBN 978-80-7400-722-4.

2.2 Historie

První kryptografický systém byl představen již v roce 1982 a byl uveden v život roku 1990 pod názvem eCash společností Digicash. Tuto revoluci zahájil David Chaum, podle Stroukala známý jako „*otec digitálních měn*“ nebo *„otec anonymní komunikace“* avšak i přes to, jak inovativní vynález eCash byl, tak nepředstavoval zásadní změnu. Ukázalo se, že není možné konkurovat státním měnám bez právních následků. Měna E-gold byla digitální měna zajištěná skutečným zlatem, které společnost nakupovala a ukládala. Vláda mohla E-gold snadno regulovat, protože znala její tvůrce a sídlo společnosti, což vyústilo k následnému soudnímu stíhání tvůrců a k ukončení existence kryptoměny. Podobný osud postihl tvůrce populárního Liberty Dollaru. V roce 2011 byl tvůrce Liberty Dollaru Bernard von NotHaus odsouzen za padělání peněz a terorismus. Podle obhajoby Bernard von NotHaus pouze reagoval na skutečnost, že americké dolary nebyly již desítky let ničím kryté (a neměly pevně stanovený limit zásoby), a proto vytvořil alternativní měnu krytou drahým kovem. Anne Tompkins, státní zástupkyně ve zmíněném případu, tvrdila u soudu, že se jedná o „*jedinečný případ terorismu*“ a že Bernard von NotHaus se měl pokusit zničit měnu své rodné země.[3]

Pseudonym Satoshi Nakamoto, který je považován za tvůrce bitcoinu, zůstává osobou, nebo skupinou osob, která nikdy neodhalila svou pravou totožnost[4], V srpnu 2008 odeslal první doložený e-mail Adamu Backovi (který jej později zveřejnil) o bitcoinovém systému, ale tehdy se mu nedostalo téměř žádné pozornosti. V říjnu téhož roku zaslal první verzi bitcoinového systému do kryptografické diskuzní skupiny, kde získal podporu od Hal Finney, kterému následně zasílal beta verze softwaru.

V lednu 2009 začal tento nový systém provozovat na několika osobních počítačích. První transakce se uskutečnila mezi Satoshi Nakamoto a Hal Finney. Dne 12 října 2009 proběhla první známá transakce za americké dolary, kdy bylo směněno 5050 BTC za 5,02 USD. Tato cena byla stanovena tak, aby odpovídala nákladům na spotřebovanou elektrickou energii při těžbě BTC, což představovalo 1000 BTC za 1 USD.

Postupem času se těžba zlepšovala. Začalo se využívat grafických karet (předchozím způsobem těžby bylo pomocí procesoru). Historicky první platba BTC za

[3] STROUKAL, D. et al. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání.* Praha: Grada Publishing 2021. 20-27 s. ISBN 978-80-271-1043-8.

[4] MACHÁČ, O. *Satoshi Nakamoto a Bitcoin.* [online] 20.11.2022. Fintree. [cit. 2023-13-10] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/satoshi-nakamoto-a-bitcoin/

reálné zboží proběhla 22. května 2010, kdy Laszlo Hanecz (programátor stojící za způsobem těžby skrze grafické karty) koupil dvě pizzy o hodnotě 50 USD za 10 000 BTC.[5]

2.3 Základní pojmy

2.3.1 Soukromý klíč

Soukromý klíč je náhodné číslo o délce 256 bitů, jeho získání lze přirovnat k metodě, kdy hodíme 256krát minci, přičemž rub zastupuje číslo 1 a líc číslo 0. V praxi se tyto klíče vytvářejí s využitím softwarových nástrojů, které používají kryptograficky bezpečný generátor pseudonáhodných čísel (CSPRNG). Soukromý klíč vytvořený tímto způsobem je zcela náhodný a pro případného útočníka je téměř nemožné jej dedukovat. Konkrétněji uhodnout celý klíč se pravděpodobnostně dá přirovnat jako vyhrát loterii 9x v řadě, nebo uhodnout jeden konkrétní atom v celém vesmíru. Jeho hlavním účelem je doložení o vlastnictví určité kryptoměny.

2.3.2 Veřejný klíč

Veřejný klíč bývá obvykle vytvořen ze soukromého klíče s využitím komplexní matematické metody známé jako kryptografie eliptických křivek, která používá standard secp256k1, jenž byl vyvinut společností Certicom Research. Následně se adresa, což je v podstatě ekvivalent bankovního účtu, odvodí jako haš (kryptografické šifrování) veřejného klíče. Tento proces odvození funguje pouze jednosměrně, což znamená, že není možné z adresy získat zpětně veřejný klíč ani soukromý klíč.[6]

2.3.3 Transakce

Transakce ve skutečnosti přesouvá vstupy transakce na výstupy transakce. Výstup transakce může být následně použit jako vstup do jiné transakce, avšak každý výstup lze použít pouze jednou. Pro provádění této operace je zapotřebí, aby všechny adresy zahrnuté do vstupů transakce byly podepsány majiteli soukromých klíčů, což je jejich způsob udělení souhlasu pro převod kryptoměn patřících vstupů do výstupu transakce.

Celkový počet kryptoměn obsažený v transakční vstupech se označuje jako transakční poplatek. Výše tohoto poplatku není pevně stanovená, ale může být nastavena

[5] LÁNSKÝ, J. *Kryptoměny.* Praha: C.H. Beck, 2018. 4-9 s. ISBN 978-80-7400-722-4.

[6] PRITZKER, Y. *Vynález jménem bitcoin.* Přeložil Tereza WONGOVÁ. Praha: Braiins Publishing, 2020. 71–77 s. ISBN 978-80-907975-0-5.

majiteli soukromých klíčů spojených s adresami v transakčních vstupech. Poplatek nesmí být záporný a nemůže přesáhnout množství kryptoměn, které byly do transakce vloženy. Možnosti nastavit nulový poplatek existuje, ale s rostoucím poplatek se zkracuje i doba jeho zpracování. Naopak, při nízkém poplatku může hrozit, že transakce nebude zpracovaná nikdy.[7]

2.3.4 Blockchain

Blockchain (Bločenka) je v podstatě digitální záznam o všech transakcích. Lze jej také nazvat internetovou účetní knihou. Transakce, které zaznamenává mohou být o různých aktivech, jako jsou fiat měny (euro, dolar, …) digitální měny, akcie, nebo jiná hodnotná aktiva. Jedním z významných aspektů blockchainu je jeho schopnost plnit širokou škálu podmínek pro nabytí nebo vypořádání těchto aktiv prostřednictvím tzv. chytrých kontraktů. Odlišností od klasické účetní knihy tkví v tom, že záznamy o transakcích jsou ukládány na několika počítačích, které tvoří decentralizovanou síť.[8] K dosažení shody v síti je potřeba aby vznikla shoda (konsensus) mezi uzly. Jakmile je shoda dosažena, každý uzel v síti aktualizuje svou vlastní kopii záznamů. Blockchain se dále dělí na jednotlivé samostatné bloky. Bloky jsou šířeny a replikovány po celé síti, čímž vytvářejí transparentní digitální účetní knihu. Samotné uzly zároveň udržují kompletní kopii záznamů, a bloků, které slouží k ukládání informací o transakcích a k jejich distribuci mezi všemi uzly v síti, soubor všech bloků je bločenka.[9]

2.3.5 Anonymita

Anonymita bývá často uváděna jako jedna z předních výhod kryptoměn, ale po důkladném zkoumání lze zjistit, že toto tvrzení platí pouze do určité míry. Kryptoměny, které mají stejnou úroveň anonymity jako Bitcoin, mají při jednotlivých izolovaných transakcích úroveň anonymity téměř absolutní. V moment, kdy se provádí větší počet vzájemně provázaných transakcí to již neplatí. Analýzou veřejně dostupných informací o aktuálním stavu kryptoměny uložených v bločence lze identifikovat soubor transakcí, kterých se zúčastnila stejná osoba. Identitu tohoto účastníka lze získat od kteréhokoliv z jeho obchodních partnerů. Je možné identifikovat skupinu adres, které jsou spojeny

[7] POPPER, D. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to neinvent money.* New York: HarperCollins Publishers, 2015. 25–28 s. ISBN 978-0-06-236249-0.

[8] LEWIS, A. *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them.* Coral Gables: Mango publishing 2021. 326–328 s. ISBN 978-1-6425-673-0.

[9] ANTONOPOULOS, A. M. *Mastering bitcoin.* Sebastopol CA: O´Reilly, 2015. 163–166 s. ISBN 978-1-449-37404-4.

s jednou pseudoidentitou. Každá pseudoidentita odpovídá jedné reálné osobě, avšak jedna reálná osoba může vlastnit více pseudoidentit.[10]

2.3.6 Fiat měna

Jedná se o fyzickou měnu, kterou vydává stát nebo jiná centrální autorita ve formě bankovek a mincí. Co tuto měnu odlišuje od tradičních komoditních peněz, jako je zlato, stříbro apod., je to, že nemá žádnou fyzickou hodnotu. Místo toho je hodnota této měny určená tím, kolik důvěry lidé a trhy vkládají do instituce, která ji vydala. Mezi přední významné faktory, které ovlivňují hodnotu fiat měny, patří zejména politická stabilita a situace vlády dané země, úroveň ekonomického růstu a inflace. Většina světových měn, včetně amerického dolaru, eura, britské libry patří do kategorie fiat měn.[11]

2.3.7 Těžba

Při těžbě kryptoměn je mnohdy uváděno, že probíhá pomocí složitých matematických úloh, ale ve skutečnosti se nejedná o příliš složité úkoly. Při těžbě se děje spíše velké množství opakujících se úkonů, které vyžadují hlavně výpočetní rychlost k jejich provedení. Těžební zařízení provádí opakované výpočty, při kterých přidávají čísla (nonce) k sadě písmen a čísle (hlavička nového bloku) a vytvářejí hash. Samotný proces přidávání čísel není matematicky složitý v takové míře, jak by se mohlo zdát. Lze ho přirovnat k zamotanému sudoku.[12]

Pro ilustraci, v roce 2014 kanál s názvem Ken Shirriff na platformě YouTube.com provedl výpočet jednoho kola hashovací funkce pouze s použitím tužky a papíru a bez jakékoliv technické pomoci. Dokázal to provést za 16 minut a následně vypočetl, že by tímto tempem dokázal vytěžit 0,67 hashe za den.[13] Oproti tomu notebooky s dvoujádrovým procesorem Atom 330 v roce 2009 svým výkonem těžily rychlostí 1,8 megahashů za vteřinu (MH/s). Tehdejší výkonnější stolní počítače s procesorem Core i7 920 dosahovaly rychlosti 19,2MH/s. S nástupem těžby pomocí grafických karet se rychlost těžby dramaticky zvýšila a dosáhla více než 100 MH/s. Následně se rychlost stále

[10] LÁNSKÝ, J. *Kryptoměny.* Praha: C.H. Beck, 2018. 57-63 s. ISBN 978-80-7400-722-4.
[11] KRISTKO, O. CH. et. al. *Krypto jednoduše: nejen o bitcoinu pro začátečníky*. Praha: Fisio/Cuddle, 2022. 51 s. ISBN 978-80-908809-0-0.
[12] KALISKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn*. Praha: IFP Publishing s.r.o., 2018. 97-99 s. ISBN 978-80-87383-71-1.
[13] Ken Shirriff. In YouTube [online] 2023-10-19. Dostupné z WWW: <https://www.youtube.com/watch?v=y3dqhixzGVo&ab_channel=KenShirriff>. Kanál uživatele Ken Shirriff

zvyšovala díky vývoji nových grafických karet a výrobou zařízení pro těžbu kryptoměn. Koncem roku 2021 lze vytěžit biliony hashů za vteřinu (EH/s.)

S nástupem zájmu o kryptoměny začaly vznikat těžební farmy, které využívají specializované zařízení pro těžbu známá jako ASIC (Application Specific Integrated Circuit). Tato zařízení se často vyrábí v Číně kvůli levné pracovní síle, elektrické energii, logistickým výhodám, dostupným materiálům apod. Jedna z největších světových firem pro výrobů ASIC zařízení je Bitmain vyrábějící zařízení Antminer. Důvodem vzniku těžebních farem byl rostoucí zájem o kryptoměny, efektivnější těžba a následný zisk. Těžební farmy bývají většinou umístěné ve výrobních halách, kde dobře cirkuluje vzduch čili je odváděno teplo vzniklé v důsledku těžby a je přiváděn ochlazený vzduch pro udržení optimální teploty zařízení, zároveň v těchto prostorách nevadil vzniklý hluk od ventilátorů a těžaři volili takové země, kde měli možnost mít levně distribuci elektrické energie potřebnou pro samotnou těžbu.[14]

2.3.8 Pool

V současném světě dominují těžbu specializovaní těžaři, kteří investovali značné finanční prostředky, často v řádu statisíců nebo milionů korun, do výkonných těžebních zařízení. Tito těžaři se sdružují do velkých skupin, které se nazývají „*pooly*“ Mezi největší těžební pooly patří Foundry USA, F2Pool, AntPool, Eligius, český Slushův pool a Poolin.[15]

Těžaři v rámci poolů se podílejí na těžbě a přidávají svou výpočetní sílu do těžby. Transakce, které generují, jsou odesílány do poolu, který je následně spravedlivě rozděluje mezi těžaře na základě jejich odvedené práce. Každý těžební pool mé své vlastní pravidla, některé účtují poplatky, zatímco jiné to nedělají. Některé sdílejí transakční poplatky s těžaři, mezitím co jiné si je nechávají. Těžaři mají možnost si vybrat pool podle svých preferencí a zájmů, což vytváří konkurenci mezi jednotlivými pooly.[16]

Existuje také samostatná těžba, ale tato možnost nese určité riziko. K získání lepší představy o tom, jak funguje těžba v poolu, uvažujme u těžaři, který disponuje těžebním výkonem takovým, jež má šanci vytěžit jeden blok s pravděpodobností 0,1 %. Pokud by

[14] KALISKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn.* Praha: IFP Publishing s.r.o., 2018. 97-99 s. ISBN 978-80-87383-71-1.
[15] PETŘÍK, J. *Těžba – mining*. [online] Btctip, 2023. [cit. 2023-10-25] dostupné z WWW: https://www.btctip.cz/tezba-mining/
[16] STROUKAL, D. et al. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání.* Praha: Grada Publishing 2021. 85–86 s. ISBN 978-80-271-1043-8.

se takový těžař připojil k poolu, který má 20 % výpočetní kapacity sítě, Tak by jeho šance na vytěžení bloku by vzrostla na 20 %. V takovém případě by těžař obdržel svůj podíl na vytěžených bitcoinech na základě svého příspěvku. Pokud by jeho výpočetní kapacita tvořila 0.5 % celkového výkonu v rámci poolu, získal by 0,065 BTC z vytěženého bloku. Tímto způsobem by v průměru získával 0,065 BTC za každých padesát minut, protože by pool vytěžil v průměru jeden blok za deset minut. Pokud by těžil sám, byl by úspěšný v průměru jednou za tisíc pokusů čili jednou za týden.[17]

2.3.9 Halving

Bitcoin byl navržen s omezením celkového počtu digitální mincí na 21 milionů. Tyto mince se uvádějí do oběhu prostřednictvím těžby, ale množství mincí, které jsou vygenerovány každý den, postupně klesá. Každé čtyři roky dochází k půlení počtu denně vytěžených nových mincí. Tato událost známá jako „*půlení*“ má zásadní význam pro vzácnost kryptoměny, a proto je očekávána držiteli kryptoměn, protože historicky pokaždé způsobila nárůst hodnoty měny. Je důležité poznamenat, že po každém půlení je zhodnocení kurzu BTC menší než v předchozích cyklech. Zároveň platí, že zvýšení hodnoty BTC bývá většinou doprovázeno růstem hodnoty ostatních kryptoměn, protože jejich ceny silně korelují s hodnotou BTC.[18]

Tabulka 1 - Vývoj ceny BTC v letech 2012-2020[19]

DATUM HALVINGU	SNÍŽENÍ ODMĚNY ZA NALEZENÝ BLOK	CENA BTC V DEN HALVINGU A PO ROCE
28.11.2012	50 BTC → 25 BTC	12,35 USD/ 1100 USD
9.7.2016	25 BTC → 12,5 BTC	637,63 USD/ 2570,88 USD
11.5.2020	12,5 BTC → 6,25 BTC	8558,18 USD/ 57 546,62 USD

[17] SASSEN, G. *Co je to ten mining pool (těžařský pool) a proč vlastně existuje?* [online] 08.11.2017. Bitcoinblog. [cit. 2023-10-25] Dostupné z WWW: https://bitcoinblog.cz/co-je-to-ten-mining-pool-tezarsky-pool-a-proc-vlastne-existuje/

[18] VÁVRA, J. *Půlení bitcoinu má poslat cenu kryptoměny do nebes. Držitelé na halving čekají čtyři roky.* [online]. 14.04.2023. E15. [cit. 2023-10-20] Dostupné z WWW: https://www.e15.cz/bitcoin-halving-2024.

[19] VÁVRA, J. *Půlení bitcoinu má poslat cenu kryptoměny do nebes. Držitelé na halving čekají čtyři roky.* [online]. 14.04.2023. E15. [cit. 2023-10-20] Dostupné z WWW: https://www.e15.cz/bitcoin-halving-2024.

2.4 Bitcoin

Bitcoin představuje digitální platidlo vytvářené a sdílené mezi jednotlivci pomocí svých počítačů. Je to měna, která nemá fyzickou podobu čili existuje pouze jako záznam v elektronické paměti počítačů, a nelze ji fyzicky získat nebo držet v ruce jako konvenční hotovost. BTC se dělí na satoshi, 1 BTC je 100 000 000 Cílem Bitcoinu je eliminovat potřebu státní regulace, zabezpečit transakce a uchovávat hodnotu v globálním měřítku mezi jednotlivci po celém světě. To přináší nové perspektivy na otázky spojené s tradičním penězi.[20]

Tradiční peníze mají aktuálně oproti Bitcoinu řadu odlišností. Jedním ze stěžejních rozdílů je to, že klasické peníze neboli fiat měny jsou centralizované, tudíž nad nimi stojí centrální autorita, která je koriguje a provozuje. V případech ekonomických kolapsů může centrální autorita vydávat do oběhu víc měny, tím se snižuje jejich hodnota a vzniká inflace. Oproti tomu Bitcoin je decentralizovaný spletitou síti v paměti počítačů, zároveň je pevně dáno kolik BTC bude vytěženo (21 milionů BTC). Tím je jeho hodnota navyšovaná kvůli vzácnosti. Hodnota BTC během své existence poměrně rapidně kolísá, čímž se stává zajímavou možností investic. Hodnota BTC dále vzlíná ze schopnosti rychlých transakcí velkého objemu hodnoty po celém světě a bezpečnosti. Pokud by určitá skupina chtěla zaútočit na BTC síť pro účel vlastního obohacení, musela by vlastnit více než 50 % těžebního výkonů, taková koordinace se aktuálně považuje za téměř nemožnou.[21]

2.5 Ethereum

Když se v roce 2012 začal zajímat rusko-kanadský programátor Vitalik Buterin o kryptoměny a zejména BTC, nedostávalo se mu příliš velké pozornosti, kritizoval určité vlastnosti, které shledával jako nedostatky. Postupně začal přispívat články do Bitcoin Magazine a navrhoval inovace pro Bitcoin. Avšak tyto nápady nenašly širší podporu v komunitě okolo BTC, což vedlo Vitalika ve vytvoření zcela nové kryptoměny. První vizi představil v roce 2013 a následující rok publikoval oficiální dokument s názvem Yellow Paper. Následně v roce 2015 vzniklo Ethereum.[22]

[20] OULEHLA, R. *Co je bitcoin? Vše stručně a přehledně v jednom článku!* [online].17.03.2021. Fintree. [cit. 2023-10-30] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/co-je-bitcoin/

[21] BARTOK, J. *Co jsou to kryptoměny? Vítejte ve světe digitálních peněz.* [online]. 13.04.2022. Portu magazín. [cit. 2023-10-30] Dostupné z WWW: https://magazin.portu.cz/co-jsou-to-kryptomeny-vitejte-ve-svete-digitalnich-penez/

[22] MACHAČ, O. *Co je to ethereum?* [online] 1.5.2021. Fintree. [cit. 2023-10-30] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/ethereum/

Ethereum stejně jako BTC využívá decentralizovanou blockchainovou technologii jako svou databázi. Nicméně se Ethereum v dalších klíčových oblastech výrazně liší. BTC byl navržen primárně jako digitální měna a online platební systém, Ethereum staví na konceptu chytrých smluv. To znamená, že vedle zaznamenávání hodnoty kryptoměny do blockchainu jsou do něj také zapsány všechny prováděny kontrakty. Tímto způsobem lze transparentně provádět finanční transakce, nakupovat akcie a uzavírat dohody bez zásahu třetích stran. A co se jednou zaznamená do blockchainu nemůže být nikdy změněno. Ethereum umožňuje uživatelům psát vlastní programy(tokeny), neboť disponuje vlastním programovacím jazykem. Ethereum tedy nabízí oproti BTC širší funkčnost. Posledním velkým rozdíl je mnohem rychlejší těžba než u BTC a fakt, že zatím nebylo vytěženo tolik jednotek Etherea jako BTC. Blockchain Ethereum má svou nejdominantnější měnu Ether.[23]

2.6 XRP

„XRP je digitální aktivum (kryptoměna) vytvořené jako most k množství dalších měn k celosvětovému použití. XRP má sloužit k tzv. internet of value, tedy tak, aby bylo možné posílat peníze stejně rychle a snadno jako dnes posíláme informace. X = ISO 4217 standard pro označení nestátních měn. RP = ze slov „ripple credits“ nebo zkráceně „ripples“[24]

Ripple Labs, firma zaměřená na inovace v oblasti finančních technologií a mezinárodních plateb, vytvořila v roce 2012 kryptoměnu XRP se zásobou 100 miliard tokenů a doprovodnou síť pro přímé mezinárodní převody peněz. Klíčovým cílem XRP je poskytovat rychlé transakce s kratší dobou potřebnou k potvrzení ve srovnání s jinými kryptoměnami, jako je například Bitcoin. Kromě toho byla XRP navržena jako nízkonákladová alternativa pro mezinárodní převody peněz, přičemž transakční poplatky obvykle jsou nižší ve srovnání s tradičními platebními systémy.[25]

[23] VOKŘÁL, J. *Zatímco bitcoin padal, ethereum rostlo. Čím se od něj liší?* [online] 30.4.2021. Seznam zprávy. [cit. 2023-10-30] Dostupné z WWW: https://www.seznamzpravy.cz/clanek/ethereum-152608
[24] KULHÁNEK, P. *XRP, vládce kryptoměn, aneb bitcoin nemá důvod k existenci.* Litomyšl: H.R.G. spol. s.r.o., 2020. 14 s. ISBN 978-80-88320-28-9.
[25] *Ripple (VŠE, CO CHCETE VĚDĚT).* [online] 04.03.2020. Alza. [cit. 2024-01-31] Dostupné z WWW: https://www.alza.cz/ripple-xrp#co-je-to

3 Kyberprostor

Hlavním pilířem fungování internetu je jeho centrální síť, která umožňuje přenos dat prostřednictvím různých přenosových médií, jako jsou datové vodiče, bezdrátové spoje a další média. Tato síť spojuje globální síť s menšími lokálními sítěmi, a to díky používání IP protokolu, což umožňuje komunikovat, sdílet informace a poskytovat různé online služby. Vytváří tak dynamický kyberprostor, který se neustále vyvíjí a nemá přesně definované hranice, ale je pevně spjat s fyzickými technologiemi v reálném světe.

Podle Koloucha je *„kyberprostor virtuální realitou, která nemá konec ani začátek, ale jeho existence závisí na technologiích a infrastruktuře v reálném světě.“* Tento paradox spočívá v tom, že kyberprostor, který se zdá být nehmotným, musí existovat díky materiálnímu světu a jeho technologickým komponentům. Pokud by však došlo k úplnému selhání materiálního média a jeho součástí, kyberprostor by mohl být nevratně narušen, případně zničen jako celek.[26]

3.1 Historie internetu

4. října 1957 Sovětský svaz vypustil na oběžnou dráhu Země svou družici Sputnik 1, tato událost byla pro USA ukázkou, jak pozadu jsou se svým vesmírným programem což šlo ruku v ruce s probíhající studenou válkou mezi USA a SSSR. Na zaostávání v kosmických technologiích navazovaly i další technologie, zejména ty vojenské, to způsobovalo bezpečnostní riziko pro USA, proto vláda začala jednat a v roce 1958 založilo ministerstvo obrany USA agenturu ARPA (Advanced Research Project Agency) zaměřenou na podporu výzkumných projektů vedoucích k novým technologiím. Agentrura ARPA měla k dispozici velkorysé podmínky, zároveň byla osvobozena od spousty administrativních úkonů čímž měli pracovníci prostor se věnovat plně své práci.[27]

3.1.1 Arpanet

Počítačová sít provozována v letech 1969-1990 se nazývala Arpanet. V samých počátcích byl její hlavní cíl primárně technický a spočíval v ověřování správného fungování systému během experimentálního přeposílání datových paketů mezi hostitelským počítačem a terminálovým serverem. První síťový protokol pro přenos dat

[26] KOLOUCH, J. *CyberCrime*, 1. Edice CZ.NIC: Praha, 2016, 43 s. ISBN 978-80-88168-34-8.
[27] *Jak na internet* [online]. 2017 [cit. 2023-10-25]. Dostupné z WWW: https://www.jaknainternet.cz/page/1205/historie-internetu/

obsahoval telnet, sloužící ke vzdálené práci na serveru, a FTP, který umožňoval přenos souborů mezi různými klienty.[28]

V počátcích existence ARPANETU byly k této síti připojeny čtyři počítače amerických univerzit v Kalifornii, Standfordu, Utahu a Santa Barbary. I přes rozdílné operační systémy mohly tyto počítače mezi sebou komunikovat. Přenos dat byl zprostředkován protokolem nazývaným NCP (Network Control Protocol). V 70. letech se ARPANET rozšiřoval a propojil více výzkumných stanic s podporou ministerstva obrany USA se povedlo vytvořit protokol TCP/IP, který položil základní kámen dnešního internetu. V roce 1980 se protokol IP stal oficiálním standardem pro americké ministerstvo obrany a ARPANET. V té době se počítače amerického ministerstva obrany oddělily od ARPANETU a vytvořily svou vlastní sít MILNET. O pár let později vznikla další hlavní páteřní síť NSFNET, kterou vytvořila National Science Foundation, vládní instituce zodpovědn**á** za vědu a výzkum v USA. V roce 1990, byla původní ARPANET síť vypnuta, protože jak vláda, tak i veřejnost přešla na modernější lepší síť.[29]

3.1.2 World Wide Web

V počátku 90. let minulého století byly klíčové prvky dnešního internetu, konkrétně protokoly síťové a transportní vrstvy, téměř kompletní. Překážkou jeho rozšíření mezi veřejnost byly dva faktory. Prvním bylo oficiální omezení internetu na akademickou komunitu, které bylo odstraněno v roce 1991 v USA a později v ostatních rozvinutých zemích. Druhým problémem byla obtížná použitelnost internetových aplikací, které byly převážně vytvářeny pro interní účely programátorů, Vznik služby World Wide Web (WWW) v ženevském Centru jaderného výzkum CERN v roce 1990 představoval skutečnou revoluci. Tim Berners-Lee a Robert Cailliau propojili základ moderního webového prohlížeče. První webový server byl spuštěn v CERNu, ačkoli původně pro vědeckou komunikaci. Milníkem se stalo dokončení prvního grafického internetového prohlížeče, Mosaic, který otevřel cestu pro masové využívání internetu díky své dostupnosti pro různé platformy osobních počítačů. Následný vývoj už spočíval pouze v globalizaci, vylepšování a rozšiřováním dostupnosti internetu.[30]

[28] *Co je ARPANET*. [online]. Správa sítě. [cit. 2023-10-31] Dostupné z WWW: https://www.sprava-site.eu/arpanet/
[29] HADRAVA, L. *Pradědečkem internetu je arpanet.* [online] ČT24. [cit. 2023-10-31] Dostupné z WWW: https://ct24.ceskatelevize.cz/svet/1387310-pradedeckem-internetu-je-arpanet

3.2 Struktura internetu

Internet se obecně dělí na 3 vrstvy, první se nazývá Surface web, který představuje veřejně dostupnou a indexovanou část internetu. Jedná se o oblast, kterou běžní uživatele snadno vyhledají pomocí běžných webových prohlížečů jako Google, Binq, Seznam apod. Jejich web crawlery navštěvují stránky, které celé prohledají, včetně odkazu na nich umístěných. Získaná data ukládají do databáze včetně adresy stránek, na kterých data získali. Na základě toho pak webové vyhledávače nabízejí relevantní informace na základě toho, co do nich bylo zadáno. Google v roce 2018 indexoval stovky miliard webových stránek. Podle odborníku tato statistika tvořila asi pouhé 4 % celého webu. Zbylých 96 % se nachází na deep webu a dark webu.[31]

Deep web představuje část internetu, která není veřejně přistupná. Tato oblast zahrnuje informační systémy vysokých škol, databáze v oblasti zdravotnictví a vládní stránky, ale také zaheslované účty, jako jsou bankovní účty, e-mailové schránky a soukromé soubory. Významným rysem deep webu je, že se obvykle nejedná o nelegální prostředí. Deep web tedy není dostupný skrze běžné vyhledávače, uživatel musí pro přístup mít buď přístupové údaje, nebo disponovat internetovým odkazem. Tímto způsobem se udržují data v bezpečí a chráněná před neoprávněným přístupem.[32]

Dark web představuje prakticky nejhlubší vrstvu internetu, lokalizovanou na darknetech, což jsou překryvné sítě integrované v rámci internetu. Charakteristickým rysem dark webu je, že k němu lze získat přístup pouze prostřednictvím specializovaného softwaru, obvykle pomocí prohlížeče TOR, zkratky pro The Onion Router. Je důležité poznamenat, že dark web je součástí deep webu, (deep web 90 % a dark net 6 % obsahu internetu) což znamená, že není indexován veřejnými vyhledávači. Uživatel musí přesně vědět, kam směřovat, aby získal přístup. Dark web bývá spojován především s nelegálními aktivitami z důvodů, že je každý uživatel v určité míře anonymní a je chráněn speciální šifrovací technologií, která směřuje uživatelská data přes několik serverů, čímž se ztěžuje sledování identity konkrétního uživatele.[33]

[31] VÁCLAVÍK, L. *Vetšina internetu je skrytá. Co jsou to deep a dark web?* [online] 8.10.2018 Cnews. [cit. 2023-11-27] Dostupné z WWW: https://www.cnews.cz/clanky/co-je-to-deep-invisible-hluboky-dark-temny-web/

[32] *Dark web a deep web aneb temná zákoutí internetu.* [online] 15.5.2023 Krytoland [cit. 2023-11-27] Dostupné z WWW: https://www.krytoland.cz/dark-web-a-deep-web-aneb-temna-zakouti-internetu

[33] ČIHÁK, L. *Co je to Dark Web, jak se na něj dostat a kam se na něm vydat?* [online] 29.11.2022 CDR [cit. 2023-11-27] Dostupné z WWW: https://cdr.cz/clanek/co-je-dark-web-jak-se-na-nej-dostat-kam-se-na-nem-vydat

Na dark webu působí řada jednotlivců, včetně umělců, disidentů, whistleblowerů a novinářů, zejména z represivních režimů, kteří čelí cenzuře na internetu nebo vyjadřují obavy ohledně ochrany svého soukromí. Díky vysoké úrovni bezpečnosti a anonymizace využívají tito lidé dark web k zajištění komunikace. Zároveň kvůli obyvatelům zemí, kde je cenzura internetu na denním pořádku provozuje své zpravodajské aktivity na dark webu například BBC, New York Times apod. Mezi českými jednotlivci jsou známí například členové skupiny Ztohoven. Zahraniční osobností, která využívala služby Toru a dark webu, byl například Edward Snowden.[34]

Po teroristických útocích z 11. září 2001 začala Národní bezpečnostní agentura (NSA) v USA sledovat komunikaci podezřelých teroristů. Ovšem v rámci tohoto sledování NSA též monitorovala komunikaci i běžných občanů, čímž se dostávala k jejich e-mailům, platebním údajům a historii internetového vyhledávání. Americké bezpečnostní služby spolupracovaly s technologickými firmami, které jim poskytovaly přístup k telefonním hovorům, mobilním telefonům a počítačům. Edward Snowden coby agent CIA se rozhodl zveřejnit tyto informace, předal třem novinářům ukázku z nasbíraných dat NSA, vybral veškeré své finance, vymazal veškerá data ze svých počítačů a sjednal si s nimi schůzku v Asii. V USA byl obviněn ze špionáže, ovšem jeho vynesení svědectví mělo velký dopad na budoucnost NSA, které je aktuálně mnohem více transparentní, USA změnilo některé ústavní zákony, aby podobná situace již nenastala. Evropská Unie vydala nařízení o ochraně osobních údaje podle nařízení GDPR. Aktuálně žije v Rusku, kde dostal i Ruské občanství.[35]

Veřejností více vnímanou stranou dark webu je ilegální činnost. Na dark webu operuje velké množství tržist, kde lze nakoupit nejrůznější zboží, Kromě získané anonymity tato tržiště ještě disponují tím, že zde neexistuje státní regulace, což znamená, že se neplatí žádné daně, ani clo. V nabídce temných tržišť se objevují zakázané položky, jako jsou drogy, zbraně, dětská pornografie, služby nájemných vrahů, falešné bankovky, padělané průkazy totožnosti, údaje k online účtům a platebním kartám (včetně CCV

[34] WAGNER, J. *Dark web – proč děti zajímá a co jim tam hrozí* [online] 15.11.2022 Pedagogicke info [cit. 2023-11-28] Dostupné z WWW: https://www.pedagogicke.info/2022/11/kybcast-dark-web-proc-deti-zajima-co.html

[35] VÁCLAVÍKOVÁ, J. *Co přineslo Snowdenovo odhalení: Šifrovaná komunikace i omezení moci tajných služeb* [online] 11.6.2023 Aktuálně [cit. 2023-11-28] Dostupné z WWW: https://zpravy.aktualne.cz/zahranici/co-prineslo-snowdenovo-odhaleni-pred-10-lety/r~ea4780ea06c611eea3c0ac1f6b220ee8/

kódů). Kromě toho se na těchto tržištích nabízejí i služby kybernetického zločinů, například prodej malwaru, ransomwaru nebo DDoS útoky.[36]

V roce 2011 vzniklo první první tržiště pojmenované jako Silk road. Založil jej Ross William Ulbricht z amerického Texasu pod pseudonymen Dread Pirate Roberts. Z počátku se jednalo o malé tržiště a jasně vymezenými pravidly. Neprodávalo se na něm žádné zboží, které by se mohlo použít k ublížení nebo podvodu, vesměs šlo tedy především o prodej drog. V internetové komunitě se poměrně rychle rozšířil, takže Ross William Ulbricht zaměstnal lidi k moderování obsahu na svém tržišti. Jako platební prostředek akceptoval Bitcoiny, obchod probíhal podobně jako posílání Bitcoinu čili veškerá komunikace byla šifrovaná, včetně plateb. Prodávající a kupující měli systém hodnocení, který se běžně používá dodnes čili škála 1-5 hvězd, přičemž plný počet znamená velký počet spokojených zákazníků nebo prodejců. Silk road měl mimo jiné i podmínku pro nové prodávající poskytnutí zálohy 500 USD, aby se vyvaroval potencionálním agentům policie nebo podvodníkům. Za svůj dvouletý provoz měl transakce za 10 000 000 BTC, přes 380 obchodníků, 1,2 milionů transakcí a 146 000 zákazníků. Policie Rosse W. Ulbrichta dopadla kvůli vlastní chybě, když najímal moderátory tak případné zájemce odkazoval skrze emailovou adresu, kde bylo napsáno jeho jméno. Během vyšetřování byl zatčen v moment, kdy měl u sebe nootebook s přihlášením administrátora na Silk Road pod účtem Dread Pirate Roberts. Byl odsouzen za prodej a pašování drog, praní špinavých peněz a hackerskou činnost, dostal trest 2x doživotí + 40 let bez možnosti podmínečného propuštění a pokutu 183 milionů dolarů. Odhaduje se, že během své činnosti vydělal 79 milionů dolarů.[37]

[36] *Největší hrozby a příležitosti dark webu.* [online] 24.10.2022 Digital Security Guide [cit. 2023-11-28] Dostupné z WWW: https://digitalsecurityguide.eset.com/cz/nejvetsi-hrozby-a-prilezitosti-dark-webu?utm_source=twitter&utm_medium=post&utm_content=dsg&utm_campaign=sc10#h2-2

[37] STREAM, 29.07.2022 *Spojil drogy s Bitcoinem a vydělal miliony. Příběh Rosse Ulbrichta.* Stream video. [cit. 2023-11-28] Dostupné z: https://www.stream.cz/ekonomie-lidskou-reci/spojil-drogy-s-bitcoinem-a-vydelal-miliony-pribeh-rosse-ulbrichta-64365225

4 Kyberkriminalita

Vzhledem k dynamickému rozvoji informačních technologií jsou identifikována nová společensky škodlivá jednání, což zvyšuje pozornost věnovanou kybernetické kriminalitě. Tento termín, odvozený od pojmu kybernetický prostor, či kyberprostor, byl původně nazýván informační kriminalitou.[38] Policie ČR definuje kybernetickou kriminalitu jako trestnou činnost prováděnou v rámci informačních a komunikačních technologií, včetně počítačových sítí. Tato kriminalita buď cílí přímo na oblast informačních a komunikačních technologií, nebo je spáchána s výrazným využitím těchto technologií jako klíčového prostředku pro její provádění.

Policie ČR monitoruje od roku 2011 počet kybernetických trestných činů. Během tohoto období byl zaznamenán trvale rostoucí trend evidovaných případů kybernetické kriminality, přičemž počet trestných činů vzrostl z 1 502 v roce 2011 na 8 417 v roce 2019.[39]

4.1 Kriminalita

Studium kriminality představuje základní směr v oblasti kriminologického výzkumu, zejména významné je poznání faktorů, které mohou poskytnout podněty pro kontrolu trestné činnosti. Prvním krokem v tomto směru je analýza a popis kriminality, pro jeho uskutečňování se využívá metody kriminální statistiky. Pro porozumění pravidelnostem v sociálním fenoménu je nezbytné nejprve pečlivě pozorovat a detailně popsat daný jev. V této souvislosti se někdy rozlišuje mezi kriminografií (kriminální fenomenologií), která zkoumá jevovou stránku kriminality, a kriminální etiologií, která se snaží vysvětlit původ a vývoj trestné činnosti. Informace o kriminalitě v dané oblasti, její vývoj v časovém horizontu a struktura, mohou být klíčové pro identifikaci příčin trestné činnosti, testování kriminologických teorií a vytváření efektivních strategií trestní politiky, což následně umožňuje hodnotit jejich účinnost.[40]

[38] *Kyberkriminalita.* [online] 01.05.2021. Krnov. [cit. 2023-11-28] Dostupné z WWW: https://www.krnov.cz/kyberkriminalita/d-37431
[39] *Kyberkriminalita.* [online] Policie ČR. [cit. 2023-12-11] Dostupné z WWW: https://www.policie.cz/clanek/kyberkriminalita.aspx
[40] *Stav, struktura a dynamika kriminality.* [online] FSPS MUNI. [cit, 2024-01-17] Dostupné z WWW: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/stav

- Rozsah kriminality

Měření stavu neboli rozsahu kriminality představuje nejčastěji používaný indikátor pro charakterizaci kriminality. Tento parametr poskytuje informace o počtu registrovaných spáchaných zločinů na konkrétním území, jako například městě, kraji nebo území celého státu, během určitého časového období. Rozsah kriminality zahrnuje činy, které jsou kvalifikovány jako trestné podle práva, ale také činy jinak trestné, kdy osoba, která spáchá tento skutek, není trestně odpovědná ze zákonných důvodů (věk, příčetnost).[41]

Graf 1: Registrovaná kriminalita v ČR 2012-2023, 2012-2023[42]a[43]

- Intenzita kriminality

Intenzita kriminality slouží k upravení rozsahu kriminality na počet obyvatel v daném sledovaném území a časovém období. Tento přístup umožňuje porovnávat různá města, kraje, nebo státy. Intenzita bývá vyjádřená prostřednictvím tzv. indexu kriminality, který se nejčastěji udává na 100 000 obyvatel v daném území. Existují dva druhy tohoto

[41] GŘIVNA, T. et. al. *Kriminologie, 4. rozšířené vydání.* Praha: Wolters Kluwer. 2014. 30 s. ISBN: 978-80-7478-614-3.
[42] *Kriminalita v ČR a EU – 2012-2022.* [online] Kurzy. [cit. 2024-02-02] Dostupné z WWW: https://www.kurzy.cz/zpravy/743260-kriminalita-v-cr-a-eu-20122022-pro-mezirocni-narust-registrovane-kriminality-v-roce-2022-mela/
[43] *Statistické přehledy kriminality za rok 2023.* [online] Policie ČR. [cit. 2024-02-02] Dostupné z WWW: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2023.aspx

indexu a to čistý index jež zahrnuje pouze obyvatele, kteří jsou trestně odpovědní a hrubý index zahrnujíc všechny obyvatele, včetně osob mladších 15 let.[44]

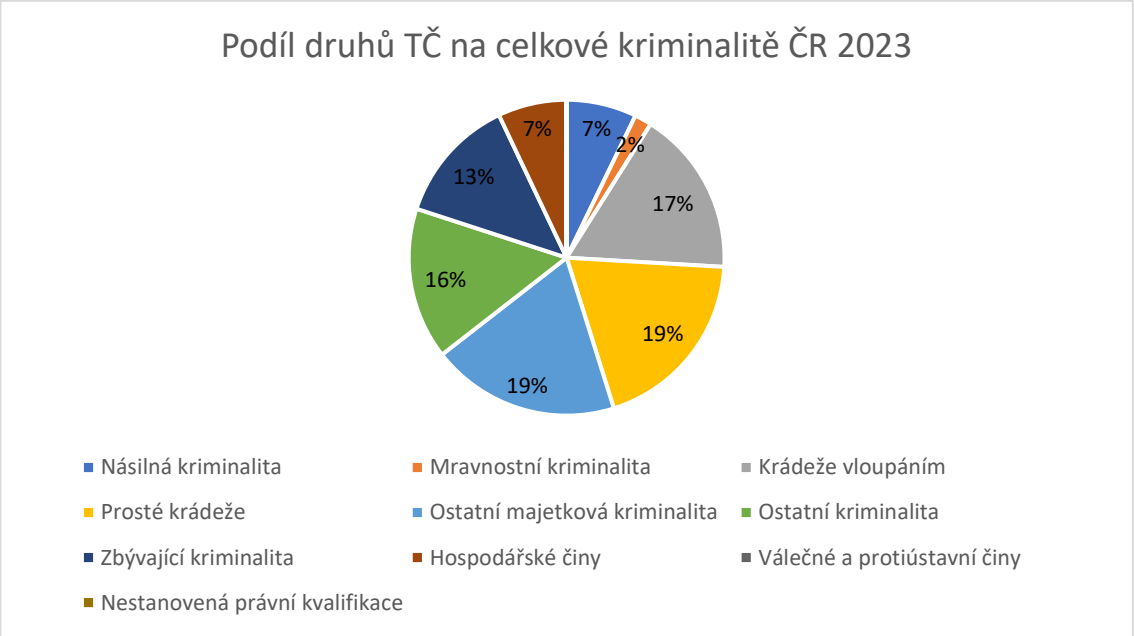
Vzorec 1: Výpočet indexu kriminality[45]

$$\frac{Počet\ trestných\ činů}{Počet\ obyvatel\ vymezeného\ území} \times 100\ 000$$

- Struktura kriminality

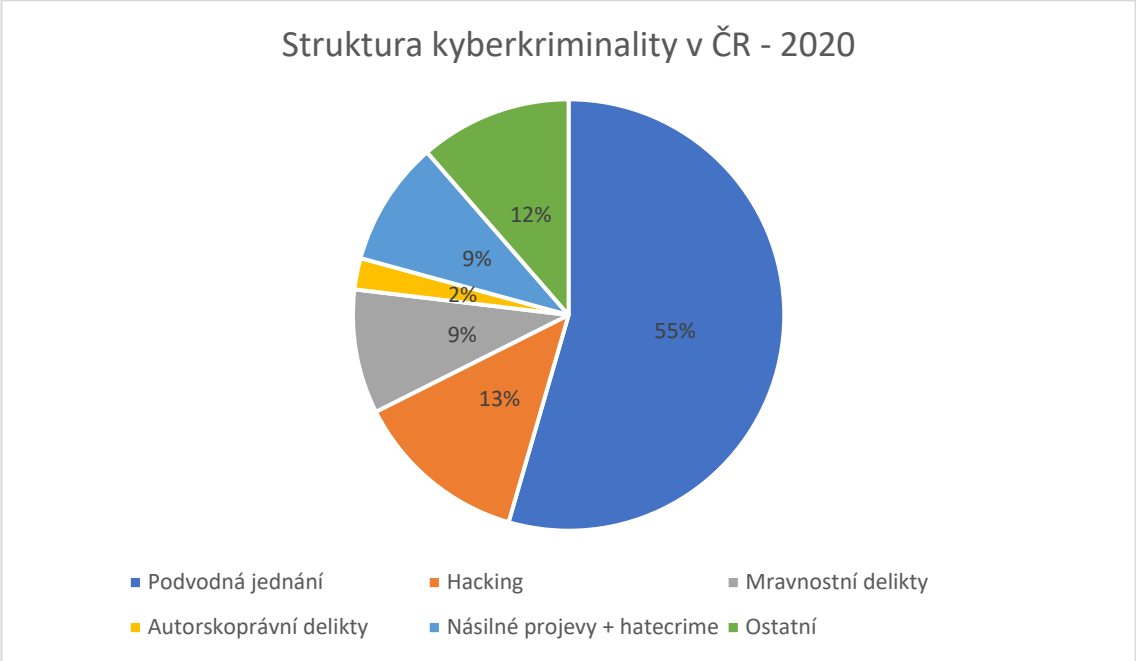
Struktura kriminality odkazuje na organizaci, rozložení, nebo složení různých forem trestné činnosti v dané společnosti, oblasti, nebo zemi. Tento koncept se zaměřuje na identifikaci a analýzu různých druhů zločinů, které se vyskytují v daném kontextu, a na jejich vzájemné vztahy. Struktura kriminality může být zkoumána z různých perspektiv, včetně typů spáchaný trestných činů, profilu pachatelů, geografického rozložení kriminality, sociálních faktorů a dalších relevantních aspektů.[46]

Graf 2: Struktura kriminality v ČR za rok 2023[47]



[44] TOMÁŠEK, J. *Úvod do kriminologie.* Plzeň: Aleš Čeněk s.r.o. 2019. 54 s. ISBN: 978-80-7380-746-7.
[45] TOMÁŠEK, J. *Úvod do kriminologie.* Plzeň: Aleš Čeněk s.r.o. 2019. 54 s. ISBN: 978-80-7380-746-7.
[46] ZAPLETAL, J. et. al. *Kriminologie, 3. vydání.* Praha: Wolters Kluwer. 2008. 57 s. ISBN: 978-80-7357-377-5.
[47] MORAVČÍK, O. *Vývoj registrované kriminality v roce 2023.* [online] 12.01.2024. Policie ČR. [cit. 2024-02-02] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx

Graf 3: Struktura kyberkriminality v ČR – 2020[48]



- Dynamika kriminality

Dynamikou kriminality rozumíme proces vývoje konání trestné činnosti v časovém horizontu. Pokud kriminalita stoupá v čase do budoucnosti jedná se o vzrůstající trend v dynamice kriminality, pokud naopak klesá, tak se na ní pohlíží jako na klesající vývoj. V případě že nestoupá a ani neklesá tak stagnuje. Zkoumání dynamiky kriminality je zejména důležité pro vypracování trendu budoucího vývoje kriminality a tím vzniká možnost ji předcházet.[49]

V roce 2022 tvořila kyberkriminalita s 18,5 tisíci případy více než 10 % celkové registrované kriminality v ČR. Meziroční nárůst byl na 94,9 %.[50] Mezi nejčastější druhy skutků patří podvody, útoky na přihlašovací údaje k bankovnictví, e-mailům, útoky skrze počítačové viry a vydírání skrze požadování výkupného za ukradené data. Podle Policie České republiky lze předpokládat, že protiprávní jednání v počítačovém prostřední bude

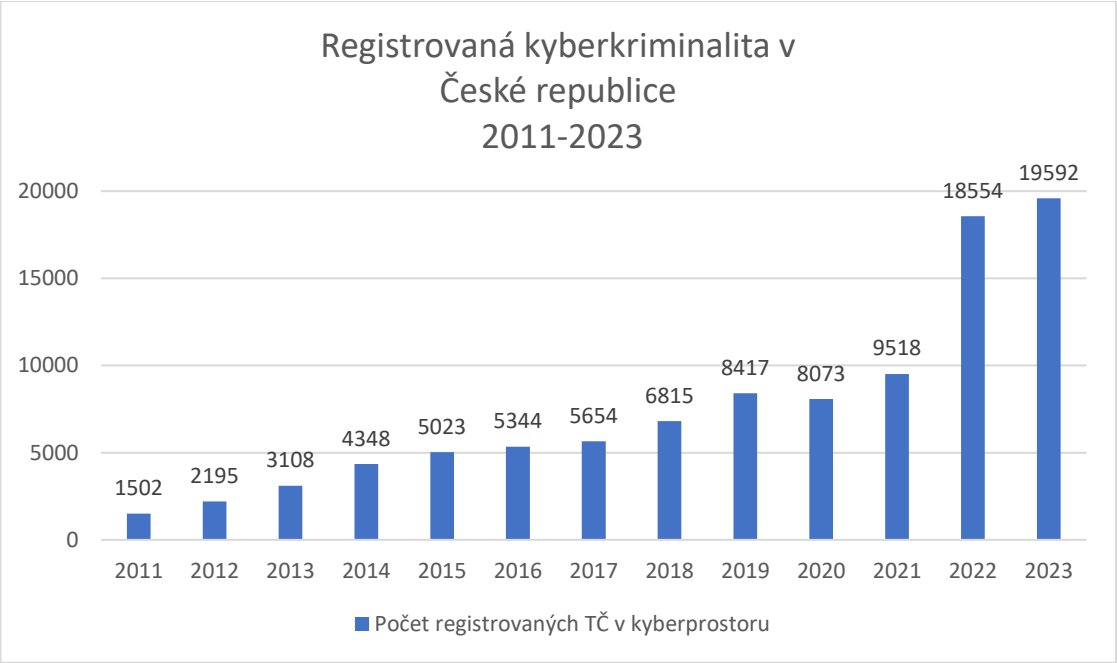
[48] *Struktura kyberkriminality 2020.* [online] Policie ČR. [cit. 2024-01-12] Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Pocitacova-mravnostni-kriminalita-%E2%80%93-kybergrooming.pdf

[49] VÁLKOVÁ, H. et. al. *Základy kriminologie a trestní politiky, 3 vydání.* Praha: C.H.Beck. 2019. 143 s. ISBN: 978-80-7400-732-3.

[50] DLUBALOVÁ, K. *Na nebezpečí kyberkriminality upozorní Den bezpečnější internetu.* [online] MVCR. [cit. 2024-01-17] Dostupné z WWW: https://www.mvcr.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx

mít v následujících letech vzrůstající charakter.[51] Za rok 2023 bylo zaznamenáno nárůst o 1 038 skutků v kyberkriminalitě, čímž se jedná o menší vzestup, než policie předpokládala.

Graf 4: Registrovaná kyberkriminalita v České republice 2011-2023[52]



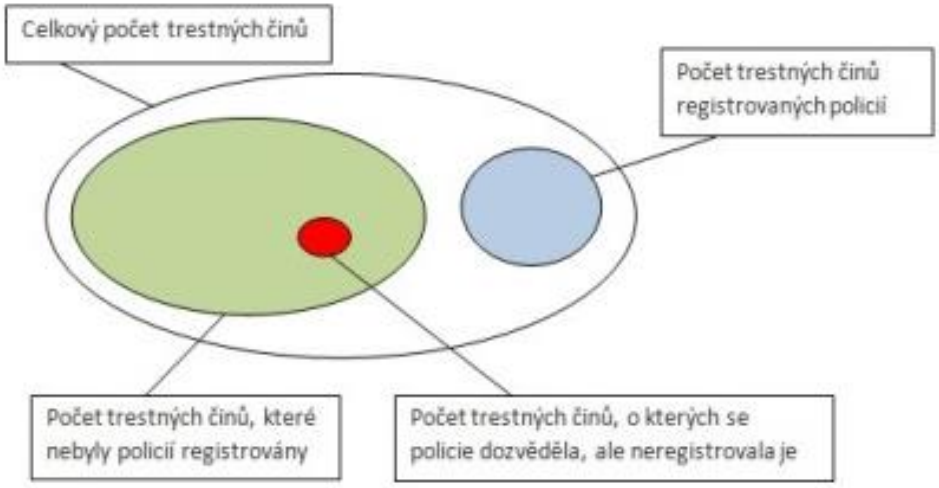
- Kriminalita skutečná, registrovaná a latentní

Registrovanou kriminalitou se rozumí taková kriminalita, o niž orgány činné v trestním řízení vědí a byla potrestaná podle trestního zákona, čili byl dopaden a usvědčen jeden, nebo více pachatelů. Latentní kriminalita neboli skrytá kriminalita jsou skutky, o kterých se orgány činné v trestním řízení nedozvěděly, známo též jako černé čísla kriminality, a také ty, které jsou známy, ale nebyly registrovány třeba pro neznámého pachatele, nedostatek důkazů atd., známé též jako šedé číslo či latence umělá. Vesměs se tedy jedná o skutky, které nebyly evidovány do statistiky. U latentní kriminality může působit vícero faktorů, oběť mnohdy nechce podat svědectví. Ku příkladu znásilněné ženy mají často postraumatickou poruchu a syndrom týrané ženy, kdy se bojí jak by na ně bylo nahlíženo, co by na to řekla veřejnost nebo se bojí následné

[51] MORAVČÍK, O. *Vývoj registrované kriminality v roce 2022.* [online] Policie ČR. 13.01.2023. [cit. 2024-01-17] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
[52] MORAVČÍK, O. *Vývoj registrované kriminality v roce 2023.* [online] Policie ČR. 12.01.2024. [cit. 2024-01-18] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx

pachatelovo reakce. Kriminalita skutečná je součet všech evidovaných i neevidovaných trestných činů.[53]

Obrázek 1: Rozdíl mezi skutečnou a registrovanou kriminalitou[54]



4.2 Právní úprava v České republice

Zákon č. 40/2009 Sb., trestní zákoník ve znění pozdějších právních předpisů a norem, uvádí tři situace, které lze kvalifikovat jako majetkové trestné činy a jejichž negativní dopady spočívají v zneužití prvků informačních systému, sítí a dat. Tyto případy zahrnují:[55]

- Neoprávněný přístup k výpočetnímu systému a nosiči informací podle § 230 trestního zákoníku,
- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných podobných dat § 231 trestního zákoníku,
- Poškození záznamu ve výpočetním systému a na nosiči informací a zásah do vybavení počítače z nedbalosti § 232 trestního zákoníku.[56]

Pomoci počítačových sítí lze páchat další druhy trestných činů v širokém spektru. Může jít o podvody, vyhrožování, vydírání, krádeže identity, zpronevěru, padělání,

[53] VÁLKOVÁ, H. et. al. *Základy kriminologie a trestní politiky, 3 vydání.* Praha: C.H.Beck. 2019. 126 s. ISBN: 978-80-7400-732-3.
[54] *Stav, struktura a dynamika kriminality.* [online] FSPS MUNI. [cit. 2024-02-02] Dostupné z WWW: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/stav
[55] *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online] NGSS. [cit, 2023-12-11] Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16
[56] ČESKO. Zákon č.40/2009 Sb., trestní zákoník

zneužívání osobních údajů, porušování autorských práv, šíření poplašných zpráv, distribuci dětské pornografie, hanobení národa, hanobení etnické rasy, podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobody apod. Mezi nejzávažnější druhy internetové kriminality se řadí organizovaná trestná činnost a kyberterorismus.[57]

Mezi další právní dokumenty, jež upravují problematiku ohledně kyberkriminality řadíme dále tyto:

- Zákon č. 2/1993 Sb., Listina základních práv a svobody,
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim,
- Zákon č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních,
- Zákon č. 127/2005 Sb., o elektronických komunikacích a jeho prováděcí vyhlášky,
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.[58]

4.3 Právní úprava EU

„Způsoby ochrany dat a informačních systému jsou dnes předmětem nejednoho vědního výzkumu, ovšem tolik technická ochrana těchto systému a dat bez právního podkladu může být neefektivní v důsledku nejasného vymezení, kam až je možno při takové ochraně zajít. V tomto kontextu se naplno projevuje nesoulad právních úprav jednotlivých států s právními úpravami států ostatních. Díky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových systému a dat nemyslitelná bez existence mezinárodního, resp. nadnárodního právního rámce, a to nejen mezi členskými státy EU, ale v celosvětovém měřítku.“[59]

[57] *Počítačová kriminalita.* [online] Můj právník. [cit. 2024-03-10] Dostupné z WWW: https://muj-pravnik.cz/pocitacova-kriminalita/
[58] POLČÁK, R. et. al. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. 90 s. ISBN 978-80-7598-045-8.
[59] KOLOUCH, J. et. al. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha. Policejní akademie České republiky v Praze, 2013. 65 s. ISBN 978-80-7251-402-1.

První snahy o regulaci nově vznikajících trestných činů nezaznamenaly výrazný úspěch, a to vzhledem k odlišnostem v právních úpravách. Některé klíčové okamžiky zahrnovaly:

- V roce 1977 se konala Konference o Kriminologických aspektech Ekonomické Kriminality ve Štrasburku, kde Rada Evropy identifikovala základní kategorie počítačové kriminality.
- Ve stejném roce byl v USA představen návrh Federálního Zákona o Ochraně Počítačových Systémů, který však nebyl schválen.
- V roce 1979 uspořádal Interpol v Paříži konferenci zaměřenou na počítačovou kriminalitu.
- V roce 1986 vytvořila skupina OECD sadu doporučení pro zefektivnění mezinárodní spolupráce a vymezení kategorií počítačové kriminality.
- V roce 1989 Rada Evropy přijala Doporučení o kriminalitě související s počítači.
- V roce 1995 Rada Evropy dále přijala Doporučení týkající se problému trestního práva spojených s informačními technologiemi.[60]

V roce 2001 vznikla na půdě Rady Evropy Úmluva o Počítačové Kriminalitě, která byla následně otevřená k podpisu v Budapešti. Česká republika se připojila k Úmluvě v roce 2005, ale ratifikace proběhla až v roce 2013. Základním záměrem Úmluvy je sjednocení definic trestných činů na poli digitální technologií, což má usnadnit jejich mezinárodní stíhání, Současně slouží jako návod pro efektivní boj s počítačovou kriminalitou.[61]

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), založená v roce 2004 a posílená Aktem EU o kybernetické bezpečnosti, aktivně přispívá k formování kybernetické politiky EU. Prostřednictvím certifikace kybernetické bezpečnosti přispívá k důvěryhodnosti produktů, služeb a procesů v oblasti informačních a komunikačních technologií. Spolupracuje s členskými státy a subjekty EU a aktivně přispívá k připravenosti Evropy na budoucí kybernetické výzvy. Agentura se zaměřuje na sdílené znalostí, budování kapacit a zvyšování informovanosti, aby společně s klíčovými

[60] POLČÁK, R. et. al. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. 443 s. ISBN 978-80-7598-045-8.
[61] FILIPOVÁ, K. *Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě.* [online] 29.8.2013 Ekonom. [cit. 2023-12-12] Dostupné z WWW: https://pravniradce.ekonom.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite

zúčastněnými stranami posílila důvěru v propojenou ekonomiku, podpořila odolnost infrastruktury Unie a zajistila digitální bezpečnost evropské společnosti a občanů.

V dnešním maximálně propojeném světě představují pachatelé kybernetické kriminality závažnou hrozbu pro vnitřní bezpečnost Evropské unie a bezpečnost jejich občanů online. Pandemie COVID-19 zdůraznila potřebu vyšší bezpečnosti v digitálním prostoru, kdy lidé stále více využívají internet pro osobní i profesionální účely. Pachatelé kybernetické kriminality využívají tuto situaci a zaměřují se zejména na společnosti působící v oblasti elektronického obchodu, elektronických plateb a zdravotnictví.[62]

4.4 Legalizace výnosů trestné činnosti pomocí kryptoměn

Dle §216 zákona č 40/2009 Sb., trestního zákoníku ve znění pozdějších předpisů se legalizace výnosů trestné činnosti vymezuje pojmem:

„Kdo ukryje, na sebe nebo na jiného převede, přechovává nebo užívá věc, která je výnosem z trestné činnosti spáchané na území České republiky nebo v cizině jinou osobou, nebo kdo takovou věc přemění v úmyslu umožnit jiné osobě, aby unikla trestnímu stíhání, trestu nebo ochrannému opatření nebo jejich výkonu, nebo kdo se ke spáchání takového trestného činu spolčí“[63]

Pod pojmem legalizace výnosů z trestné činnosti, známé též jako „legalizace výnosů“, „praní špinavých peněz“, se rozumí záměrně jednání, jehož cílem je zakrýt nezákonný původ jakéhokoli výnosu z trestné činnosti a současně vytvářet zdání, že tyto finanční prostředky pocházejí z legálních zdrojů v souladu s platnými zákony.

Toto jednání, podle zákona č. 253/2008 Sb. O některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, může zahrnovat následující aktivity:

- Přeměna nebo převod majetku: Úmyslná přeměna nebo převod majetku s vědomím, že pochází z trestné činnosti, za účelem jeho utajení nebo zastření původu nebo za účelem napomáhání osobě účastnící se trestné činnosti uniknout důsledkům svého jednání.

[62] SEDLÁK, P. et. al. *Kybernetická (ne)bezpečnost.* Brno. Akademické nakladatelství CERM. 2021. 66-68 s. ISBN 978-80-7623-068-2.
[63] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník

- Utajení nebo zastření povahy majetku: Skrývání nebo zakrývání skutečné povahy, zdroje, umístění, pohybu majetku nebo nakládání s ním s vědomím, že pochází z trestné činnosti
- Nabytí, držení nebo používání majetku: Nabytí, držení nebo používání majetku s vědomím, že pochází z trestné činnosti.
- Zločinné spolčení nebo součinnost: Účast ve zločinném spolčení nebo jiné formě součinnosti za účelem výše uvedených nelegálních činností.

Výnosem z trestné činnosti se pak rozumí jakákoli ekonomická výhoda z činnosti, která vykazuje znaky trestného činu.[64]

Jednou z metod legalizace výnosů z trestné činnosti může být skrze kryptoměny. Na internetové inzerci, sociálních sítích a fórech se objevují podvodné reklamy na kryptoměnové burzy. Po projevení zájmu o tyto služby bude osoba kontaktovaná falešným bankéřem, finančním poradcem apod. načež pod záštitou falešné kryptoměnové investiční platformy se uživatel následně může dopustit trestného činu legalizace výnosů z trestné činnosti z nedbalosti tím, že provede domnělý vklad, přičemž mu bude řádově během pár dní vyplacen zisk. Tento zisk ve skutečnosti nesouvisí s investicí do kryptoměnového portfolia, pouze zločinci získáním k bankovnímu přístupu mohou tento účet použít k legalizaci výnosů TČ a následně je posílat dál dle své potřeby. Uživatel se tímto ale stal pachatel stejného TČ z nedbalosti a může být proti němu zahájeno trestní řízení.[65]

Dle § 217 zákona č. 40/2009 Sb., trestního zákona ve znění pozdějších předpisů je legalizace výnosů z trestné činnosti z nedbalosti vymezena jako:

„Kdo jinému z nedbalosti umožní zastřít původ nebo zjištění původu věci ve větší hodnotě, která byla získána trestným činem spáchaným na území České republiky nebo v cizině, nebo jako odměna za něj, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci.“[66]

[64] KALABIS, Z. *Vysvětlení pojmu „legalizace výnosů z trestné činnosti“* [online] 11.11.2015. Zlatá koruna. [cit. 2023-12-26] Dostupné z WWW: https://www.zlatakoruna.info/zpravy/vysvetleni-pojmu-%E2%80%9Elegalizace-vynosu-z-trestne-cinnosti%E2%80%9C

[65] HOKROVÁ, V. *Legalizace výnosů z trestné činnosti z nedbalosti.* [online] 25.2.2022. Policie ČR. [cit. 2023-12-26] Dostupné z WWW: https://www.policie.cz/clanek/archiv-zpravodajstvi-zpravodajstvi-2022-legalizace-vynosu-z-trestne-cinnosti-z-nedbalosti.aspx

[66] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník

Samotná legalizace výnosů z trestné činnosti lze páchat pouze pomocí dlouhé řady kryptoměnových transakcí, kdy se pachatel spoléhá, že díky anonymizaci nebude odhalen. Ovšem v technologii blockchainu zůstávají data o všech transakcích čili nelze s jistotou tvrdit, že by se jednalo o zcela bezpečnou metodu. Podle Jarka Jakubčeka, bezpečnostního kryptoměnového analytika směnárny Binance, tkví jedna ze stěžejních předností při odhalování těchto zločinů právě v blockchainu. Tím že je veřejný, může jakýkoliv uživatel upozornit na transakce, které se mu zdají podezřelé. Společnost Chainalysis ve své zprávě uvedla, že 0,15 % veškerého objemu kryptoměn se dá prokazatelně spojit s kriminální činností. I přes relativně nízké zlomky procenta se to projeví v miliardách USD. Pokud se pachatelé rozhodnout legalizovat finance získané z trestné činnosti prováděné třeba prodejem drog, samotná směna na kryptoměnu a následná směna zpět na konvenční měnu k legalizaci stačit nebude. Zároveň směnárna Binance má v podmínkách uvedenou povinnost ověřit totožnost při využívání jejich služeb. Pokud se směnárně bude zdát nějaká transakce škodlivá, nemůže ji sice přerušit, ale může dané účty zmrazit a poskytnout veškerá data policii, aby tuto činnost prověřila. Jakubček dále uvádí, že směnárna dostává i několik požadavků týdně od policie o různých investičních podvodech. Většinou si policisté vyžádají data o účtech, jež jsou s těmito podvody spojené.[67]

4.5 Podvody pomocí kryptoměn

Aktuálně existuje početná variace způsobu, jak někoho podvést pomocí kryptoměn, přičemž se může jednat o odlišné metody, ale výsledek zůstává stejný a sice, že poškozený přijde o své data, nebo finance, ať už v klasické fiat měně, případně kryptoměny. Mezi pár metod patří např. tyto:[68]

- Telefonický/internetový poradce nabízející veliké zhodnocení: Falešný zástupce obchodní platformy kontaktuje oběť a nabízí pomoci psychického nátlaku možnost zhodnocení financí. Může se představit jako zástupce známé platformy, či případně její skutečný zaměstnanec. Po zaplacení určité vstupní investiční sumy může následovat přístup do

[67] ALI, S. *Peníze přes kryptoměny vyprat lze, záznam ale zůstane navždy, říká expert.* [online] 15.01.2023. iDnes. [cit. 2024-01-30] Dostupné z WWW: https://www.idnes.cz/ekonomika/zahranicni/binance-jarek-jakubcek-kryptomeny-prani-spinavych-penez.A230108_123335_eko-zahranicni_alis

[68] FANTA, M. *Znáte nejčastější kryptoměnové podvody?* [online] Cyberblog. [cit. 2024-01-30] Dostupné z WWW: https://cyberblog.cz/crypto/znate-nejcastejsi-kryptomenove-podvody/?gad_source=1&gclid=CjwKCAjw17qvBhBrEiwA1rU9w23zJ80jxKDBKFc1iJtiVWcU69PPx_ft0jHDfZ1VQ1Bi70XGBG6zFRoCtNgQAvD_BwE

falešného systému ukazujíc návratnost investice. V moment, kdy poškozený přestane investovat, nebo se pokusí investice vybrat podvodníci přestanou komunikovat. Stejným způsobem je provozován podvod, kdy pachatel poškozeného osloví, že na zapomenuté platformě má velké množství investic, nebo kryptoměn a k získání přístupu musí zaplatit aktivační poplatek, nebo daň. Výsledkem je buď ztracení všech poskytnutých financí, nebo ztráta všech prostředků na účtu, případně do limitu pro internetové platby. Škody bývají v rozmezích deseti tisíců až sto tisíců korun na skutek.[69]

- Platba za zboží na bazarových portálech: Podvodný prodejce požaduje platbu předem (případně část platby) přes určitý kryptoměnový token (nejčastěji Bitcoin), nebo pošle QR kód, kde bude v poznámce uvedeno, že se jedná o nákup kryptoměny. Platba dále jde na kryptoměnovou směnárnu, kde provede konverzi z Kč na kryptoměnový token a následně se odešle na krypto peněženku podvodníka a ten přeruší veškerý kontakt. Škody bývají v rozmezí stovek až tisíců korun na skutek.[70]
- Investice do bezcenné kryptoměny: Při tomto typu podvodu se pokouší pachatelé využít neznalosti investorů a přimět je vložit své prostředky do tokenu, který je bezcenný. Mohou využít nějakého aktuálního fenoménu, např. Squid Game je token, který využil úspěchu stejnojmenného seriálu v roce 2021. Seriál se těšil velké popularitě díky čemuž mnoho fanoušků vkládalo do tohoto tokenu své finanční prostředky, během pár dní měl tento token růst v tisících procentech, pak jeho autoři s vydělanými penězi zmizeli a token se stal bezcenným. Odhadované škody jsou v miliónech USD.[71]
- Dvojnásobek BTC: Tento typ podvodu útočí na emoce, podvodník se vydává za veřejně známou osobu, jako je třeba Elon Musk, Bill Gates, investiční influencery apod. a s příslibem, že chce konat dobrou věc slíbí, že po zaslání určitého množství BTC na svou peněženku odešle

[69] ŠPITÁLSKÁ, P. *Žena naletěla podvodníkovi. Na falešné investice do kryptoměny si vzala půjčku*. [online] 18.03.2023. Deník. [cit. 2024-01-30] Dostupné z WWW: https://berounsky.denik.cz/zlociny-a-soudy/zena-naletela-podvodnikovi-na-falesne-investice-do-kryptomeny-si-vzala-pujcku-20.html

[70] *Nejčastější podvody s Bitcoinem*. [online] 09.01.2024. Finex. [cit. 2024-01-30] Dostupné z WWW: https://finex.cz/nejcastejsi-podvody-s-bitcoinem-na-toto-si-dejte-pozor/

[71] *Utekli se 75 miliony. Kryptoměna squid těžící z popularity seriálu Hra na oliheň byla obrovský podvod*. [online] 11.02.2021. iRozhlas. [cit. 2024-01-30] Dostupné z WWW: https://www.irozhlas.cz/zpravy-svet/kryptomena-squid-hra-na-olihen-podvod-krypto-trh-kradez-75-milionu_2111021206_vis

dvojnásobnou částku okamžitě zpět. Poškození v domněnce, že by veřejně známá osoba nelhala tak učiní a o celou částku přijdou.[72]

- Phishing útoky: Poškozený si při hackerském útoku nainstaluje na svůj nosič (PC, mobilní telefon, tablet) škodlivý software. Ten může na pozadí těžit kryptoměny, čímž zařízení zpomaluje, spotřebovává více elektrické energie a více se opotřebovává, může získat citlivé údaje, nebo může nainstalovat infikovanou aplikaci, která se tváří jako kryptoměnová peněženka a po udělení soukromého klíče odešle veškeré kryptoměny na adresy podvodníků.[73]

4.6 Financování terorismu

Terorismus je politicky motivovaný násilný čin nebo hrozba násilím, který má za cíl vytvořit strach, paniku nebo nuceně ovlivnit chování lidí nebo vlád. Tyto aktivity jsou obvykle prováděny skupinami nebo jednotlivci, kteří chtějí dosáhnout politických, náboženských nebo ideologických cílů tím, že budou útočit na civilisty, vládní instituce nebo jiné symboly moci. Teroristické útoky mohou být prováděny bombovými útoky, únosy, útoky na veřejná místa, sabotáže a další formy násilí. Motivace za teroristickými činy se mohou lišit od snahy o nezávislost a autonomii až po propagaci ideologických názorů nebo odvety za nějaké události.[74]

Podle § 312d zákona č. 40/2009 Sb., trestního zákoníku ve znění pozdějších předpisů je financování terorismu vymezeno jako:

„(1) Kdo sám nebo prostřednictvím jiného finančně nebo materiálně podporuje teroristickou skupinu, jejího člena, teroristu nebo spáchání teroristického trestného činu, trestného činu podpory a propagace terorismu (§ 312e) nebo vyhrožování teroristickým trestným činem (§ 312f) anebo shromažďuje finanční prostředky nebo jiné věci v úmyslu, aby jich bylo takto užito, bude potrestán odnětím svobody na tři léta až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku.

[72] PILICI, S. *Don't Fall for the Double Your Bitcoin Scam Stealing Crypto.* [online] 02.11.2023. Malwaretips. [cit. 2024-01-30] Dostupné z WWW: https://malwaretips.com/blogs/double-your-bitcoin-scam/

[73] GREGOR, M. *Nejtypičtější krypto podvody: Na tyto věci si dávejte extra pozor!* [online] 19.02.2023. Kryptonovinky. [cit. 2024-01-30] Dostupné z WWW: https://www.kryptonovinky.cz/krypto-podvody/

[74] *Definice pojmu terorismus.* [online] 29.07.2009. MVCR. [cit. 2024-01-31] Dostupné z WWW: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx

(2) Odnětím svobody na pět až patnáct let, popřípadě vedle tohoto trestu též propadnutím majetku, bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) jako člen organizované skupiny,

b) za stavu ohrožení státu nebo za válečného stavu, nebo

c) ve velkém rozsahu.“[75]

Terorismus se financuje různými způsoby, jedním z nich může být geografická pozice jejich působení, pokud mají na svém území určité zdroje, jako je třeba nerostné bohatství, mohou je využívat pro získání zisku. Dále získávají peníze trestnou činností jako může být prodej drog, vydírání, obchod s lidmi apod. V neposlední řadě mohou získávat prostředky podporou od států, politických entit nebo formou sbírek, kde přispívají sympatizanti.[76]

Pro darování příspěvků od organizací, nebo sympatizantů nacházejících se v jiném místě světa mohou být využité kryptoaktiva. Moskevská kryptoburza Garantex je zapsaná na americké černé listině. Měla by sloužit zejména k legalizaci výnosů z trestné činnosti, obcházení sankcí vzniklých kvůli válce na Ukrajině a jako páteřní burza pro teroristické skupiny, například Hamás. Izrael zabavil adresy peněženek, u nichž má podezření, že by mohly být napojeny na teroristické či jiné militantní skupiny v hodnotě desítek milionů USD.[77]

Problémem vystopování a zmrazení účtu jsou plně decentralizované kryptoburzy, kde technologie blockchain může být skrytá. Ovšem teroristické skupiny sdíleli na svém telegramové účtu adresy kryptopeněženek, kam zasílat dary. Tím se se úřady dostaly k informaci, jaké přesné adresy odstavit a zmrazit. Zároveň získali další adresy, které byly na to napojené, jako jsou adresy přispěvatelů a dalších účtu, co sloužili k legalizaci těchto výnosů. Na druhé straně hrozbou jsou ty adresy a transakce, jež proběhnou skrytě a o kterých se úřady nedozví. Izraelský Národní úřad pro boj proti financování terorismu

[75] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník

[76] SMOLÍK, J. *Financování terorizmu.* [online] 2017. Vojenské rozhledy. [cit. 2024-01-31] Dostupné z WWW: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-prostredi/financovani-terorizmu

[77] DEYL, D. *Kryptoburza, íránci i západ: kde bere hamás peníze?* [online] 01.11.2023. Týdeník hrot. [cit. 2024-01-31] Dostupné z WWW: https://www.tydenikhrot.cz/clanek/kryptoburza-iranci-i-zapad-jak-se-financuje-hamas

zmrazil desítky kryptoměnových účtu, které byly organizací napojené pouze na Hamás. Prostředky se počítají v desítkách milionů USD a byly v tokenu Tether v síti Tron.[78]

[78] WOLF, K. *Kryptoměny ve službách teroru?* [online] 18.10.2023. Lupa. [cit. 2024-01-31] Dostupné z WWW: https://www.lupa.cz/clanky/kryptomeny-ve-sluzbach-teroru/

5 Kybernetická bezpečnost

„Kybernetická bezpečnost v posledním desetiletí získala na významu a stala se tak jednou z hlavních priorit v mnoha národních politikách. Je tomu zejména díky přesahu do jiných bezpečnostních sfér a taktéž díky incidentům, které tento pojem nechvalně proslavily a přiměly i širokou veřejnost přemýšlet o potřebě zabezpečení v kyberprostoru. S tím souvisí potřeba chránit kyberprostor tak, aby v nejvyšší možné míře byla zachována komplexní bezpečnost České republiky a zároveň práva jedinců na informační sebeurčení.“[79]

Kybernetickou bezpečnost je možné vysvětlit jako souhrn opatření a strategií, zahrnující právní, organizační, technické a vzdělávací prvky, s cílem zabezpečit ochranu počítačových systémů, aplikací, dat a uživatelů. Tyto opatření mají za úkol zlepšit schopnost počítačových systému a poskytovaných služeb reagovat na kybernetické hrozby a útoky, stejně jako minimalizovat následky těchto událostí. Zahrnuje také plánování funkčnosti počítačových systémů a souvisejících služeb po incidentu. Realizace kybernetické bezpečnosti probíhá jak v kyberprostoru, tak i mimo něj. Je důležité neomezeně aplikovat uvedené principy a prostředky bez geografických omezení.[80]

5.1 Bezpečnostní opatření uživatele

Zabezpečovací opatření lze jednoduše definovat pomocí čtyř základních bodů, které představují klíčové prvky ochrany zařízení v online prostředí. Tato opatření jsou obecná a doporučována pro každého uživatele informačních a komunikačních technologií. Nicméně, tyto preventivní kroky lze rovněž aplikovat i v podnikovém prostředí, avšak je třeba je rozšířit a aplikovat potřebám firmy. Jedná se o následující prvky: Firewall, ochrana proti škodlivému softwaru, používání silných hesel a pravidelné aktualizace.[81]

- Firewall je bezpečnostní zařízení nebo software navržený k monitorování a kontrolnímu filtrování příchozí a odchozí síťové komunikace na základě definovaných pravidel. Jeho hlavním účelem je chránit prostředí před neoprávněným přístupem, útoky z internetu a škodlivým obsahem. Firewall

[79] *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online] 30.5.2017 NUKIB. [cit. 2023-12-19] Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/
[80] KOLOUCH, J. et. al. *Cybersecurity*. Praha. Edice CZ.NIC. 2019. 42-43 s. ISBN 978-80-88168-31-7.
[81] KOLOUCH, J. *CyberCrime*, 1. Edice CZ.NIC. Praha, 2016, 61-62 s. ISBN 978-80-88168-34-8.

může být implementován jako hardwarové zařízení nebo softwarová aplikace běžící na serveru nebo síťovém zařízení. To umožňuje uživatelům kontrolu nad síťovým provozem a umožňují nastavit pravidla pro povolení nebo blokování určitých typů komunikace na základě bezpečnostních politik organizace.[82]

- Antimalware je softwarový nástroj navržený k detekci, blokování a odstraňování škodlivého softwarů z počítačových sítí. Antimalware chrání uživatele před různými druhy hrozeb, jako jsou viry, červi, trojské koně, ransomware, spyware, adware a další formy škodlivého kódu. Antimalwarové programy obvykle provádějí pravidelné skenování systému a porovnávají ho s databází známých škodlivých kódů, aby identifikovaly a odstranily potenciálně nebezpečné soubory nebo aplikace. Tím pomáhají uživatelům udržovat svá zařízení bezpečná a chráněná před kybernetickými hrozbami. Antimalware může být považován za doplněk k firewallu, bývá označován také jako antivir.[83]
- Volba dostatečné silného hesla je dalším důležitým aspektem bezpečnosti v kyberprostoru. Mezi zásady při tvorbě silného hesla patří použití malých a velkých písmen, čísel a speciálních znaků, při nejlepším nevolit slova, alespoň 8 znaků. Uživatel by měl rozlišovat 3 okruhy, jak heslo bude používat, a to je pro vstup do zařízení (počítač, telefon, wifi) vstup do soukromí (mailový účet, sociální sítě, cloud) a ostatní (internetové obchody, fóra, online hry), zároveň by měl používat různá hesla a měnit je. Existují specializované programy, jež dokáží prolomit slabé heslo během pár vteřin.[84]
- Aktualizace celého systému, ale i částí softwaru je klíčová. Tím, jak se ICT vyvíjí, tak se vyvíjí i bezpečnostní hrozby. Pro útočníky je mnohem snazší napadnout systém bez bezpečnostních záplat případně pracující na zastaralém softwaru než systémy aktualizované.[85]

[82] *Co je brána Firewall?* [online] Microsoft. [cit. 2024-02-07] Dostupné z WWW: https://support.microsoft.com/cs-cz/office/co-je-br%C3%A1na-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603

[83] *Co je to antimalware a firewall a proč je používat?* [online] 14.02.2017. Vim kam klikam. [cit. 2024-02-07] Dostupné z WWW: https://www.vimkamklikam.cz/rady-a-tipy/co-je-to-antimalware-a-firewall-a-proc-je-pouzivat

[84] KOHOUT, R. *Bezpečnost v online prostředí.* Karlovy Vary: Biblio Karlovy Vary, 2016. 18 s. ISBN978-80-260-9543-9.

[85] *5 důvodů, proč aktualizovat software.* [online] 26.09.2019 Evropská unie. [cit. 2024-02-07] Dostupné z WWW: https://portaldigi.cz/5-duvodu-proc-aktualizovat-software/

5.2 Kybernetické útoky

Kybernetický útok je snaha o neoprávněný vstup do počítačového systému, sítě, nebo jiného digitálního prostředí s cílem způsobit škodu. Tato škoda může zahrnovat deaktivaci zařízení, odcizení dat, nebo jejich zničení, a využití napadeného systému k dalším útokům nebo kontrole nad infastrukturou. Kybernetické útoky mohou být prováděny jednotlivci nebo organizacemi, včetně hackerů, hacktivistů nebo státních aktérů. Motivací pro tyto útoky může být různorodá, zahrnující vydírání, politicky motivované útoky, kyberterorismus nebo osobní prospěch, V mnoha případech mohou být útočníci motivování k získání výkupného, často vyžadovaného v kryptoměně pro zvýšení své anonymity.[86]

5.2.1 Malware

Termín malware vznikl spojením anglických slov malicious (zlomyslný) a software a poukazuje na záměr autora takového programu spíše než na jeho specifické vlastnosti. Tato kategorie zahrnuje různé formy škodlivého softwaru, jako jsou počítačové viry, červi, trojské koně, crimeware, špehovací software, vyděračský software a reklamní software. Na tvorbu malware jsou najímány specializované týmy odborníků, kteří neustále vytvářejí sofistikovanější metody pro získání hodnotných firemních nebo osobních citlivých dat. Malware se vyvíjí tak rychle, že systém, schopný se bránit pouze známým hrozbám, je téměř bezmocný,

Když malware pronikne do systému, může způsobit škody dle svého určení nebo instalovat další moduly s odlišnou funkcionalitou. Příkladem může být backdoor, který umožňuje útočníkovi opakovaný přístup k napadenému počítači a využívání ho k dalším škodlivým činnostem. Ransomware cíleně uzamkne nebo zašifruje data na napadeném zařízení a slibuje jejich obnovení pouze po zaplacení určité finanční částky v konkrétním čase a způsobem, buď prostřednictvím kryptoměny nebo online platby určitými kartami.[87]

- Trojský kůň v ICT technologii se odkazuje na příběh ze starověkých bájí. Je to druh škodlivého softwaru, který se tváří jako legitimní aplikace nebo soubor, ale ve skutečnosti skrývá škodlivý kód. Tento kód může umožnit

[86] *Co je kybernetický útok.* [online] 13.09.2022. Legislativa. [cit. 2024-02-08] Dostupné z WWW: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

[87] POŽÁR, J. et. al. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.* Praha. Policejní akademie ČR. 2020. 37-38 s. ISBN 978-80-7251-505-9.

útočníkovi vzdálený přístup k cílovému počítači, ukrást citlivá data a provádět další škodlivé činnosti na napadeném systému. Mohou být distribuovány různými způsoby jako jsou emailové přílohy, stažení z prostředí internetu, využíváním softwarových zranitelností systému nebo skrze mediální nosič jako USB flash disk, Blue-ray disk apod.[88]AIDS trojan je jeden z prvních druhů trojského koně z roku 1989. Poštou byly distribuovány počítačové diskety, jež měly mít ve své paměti důležité informace i nemoci AIDS. Po instalaci se po 90 cyklech vypnutí počítače zašifroval soubory v PC a požadoval zaplacení výkupného ve výši 189 nebo 378 USD na adresu poštovní schránky v Panamě.[89]

- Botnet je síť počítačů nebo zařízení, které jsou infikovány škodlivým souftwarem a jsou ovládány útočníkem na dálku, převážně pomocí příkazů z centrálního řídícího serveru. Tato síť je obvykle vytvořena tím, že útočník infikuje mnoho počítačů pomocí malware a následně je řídí prostřednictvím „zombie“ počítačů. Následně botnet skrze infikované počítače může distribuovat spam, škodlivý software, DDDoS útoky pro výpadky sítě a krást citlivá data.[90]

5.2.2 Sociální inženýrství

Sociální inženýrství je technika, kterou útočníci využívají k získání citlivých informací, nebo provádění neoprávněných akcí tím, že využijí lidské psychologie a sociálního chování. Namísto využití technických zranitelností se sociálním inženýrství zaměřuje na manipulaci s lidskými emocemi, důvěrou a nedostatkem povšimnutí, aby dosáhlo svých cílů. Toho může být dosaženo skrze podvodné telefonáty, kdy se útočníci přes falešnou legitimaci snaží nalákat oběť, aby poskytla citlivé informace, hesla, bankovní údaje, apod.[91]

- Pro potřeby sociálního inženýrství se využívá Phishing což je forma kybernetického útoku, který je zaměřen na získání citlivých informací od uživatele. Tento útok je obvykle prováděn pomocí podvodných telefonátů,

[88] *Co je trojský kůň.* [online] Správa sítě. [cit. 2024-02-09] Dostupné z WWW: https://www.sprava-site.eu/trojsky-kun/
[89] *Trojský kůň.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/trojsky-kun/
[90] RZYMAN, T. *Co je botnet?* [online] 27.10.2017. IP Technik, [cit. 2024-02-09] Dostupné z WWW: https://iptechnik.cz/co-je-botnet/
[91] *Sociální inženýrství.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/

e-mailů, textových zpráv nebo webových stránek, které se tváří jako legitimní komunikace od důvěryhodného zdroje, jako jsou banky, instituce, vládní úřady apod. Využívají se psychologické nástroje pro zvýšení šance na úspěšnost útoku např. falešný e-mail od banky může tvrdit, že uživatele musí okamžitě aktualizovat své údaje nebo změnit heslo kvůli podezřelé aktivitě na jejich účtu.[92]

[92] *Phishing.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/phishing/

6 Praktická část

Používání kryptoměn jako prostředku k uskutečňování nelegálních transakcí se stalo záležitostí zájmu a diskuse v kontextu finanční kriminality a kybernetických hrozeb. Od začátku existence kryptoměn se tyto digitální aktiva staly předmětem zájmu jak legálních, tak nelegálních aktérů.

6.1 SWOT matice

Tato SWOT matice se snaží zhodnotit vnitřní a vnější faktory, které ovlivňují využití kryptoměn jako platidla při nelegálních činnostech. Před samotnou analýzou lze definovat základní pojmy:

Síla (Strengths): Tyto faktory označují vnitřní aspekty kryptoměn, které mohou být považovány jako silné stránky. Mohou to být například anonymita plateb, rychlost transakcí, šifrování atd.

Slabost (Weaknesses): Slabé stránky spojené s používáním kryptoměn mohou zahrnovat výkyvy hodnoty, neregulovaný trh atd.

Příležitost (Opportunities): Externí faktory, které mohou být k posílení využití kryptoměn. Může to být technologický pokrok, rostoucí popularita kryptoměn atd.

Hrozba (Threats): Rizika spojená s používáním kryptoměn jako jsou tlak na regulaci, umělá inteligence atd.

Tato analýza poskytne podrobný pohled na výzvy a příležitosti, které kryptoměny přinášejí.

Tabulka 2 - SWOT matice

SILNÉ STRÁNKY	**SLABÉ STRÁNKY**
Anonymita transakcí Technologie blockchain Globální dosah Rychlost transakcí Nízké transakční poplatky Šifrování	Vysoká volatilita Omezená akceptace Neregulovaný trh Energetická náročnost
PŘÍLEŽITOSTI	**HROZBY**
Technologický pokrok Nárůst uživatelů kryptoměn Digitalizace měny	Regulační zásahy Negativní veřejné mínění Umělá inteligence

6.1.1 Silné stránky

- Anonymitu transakcí lze považovat jako silnou stránku, sice se nejedná o naprostou anonymitu, při běžných transakcích může být identita zúčastněných skrytá. Při nelegálních činnostech záleží na zkušenostech zločinců, za předpokladu, že si jsou vědomi, jak anonymitu využít a použijí velké množství falešných či umělých transakcí, tak se tím jejich míra anonymity zásadně zvyšuje a pro vyšetřovatele to představuje komplikaci v potírání těchto trestných činů. Dalším způsobem může být využívání sítí blockchainu, jež nejsou transparentní.
- Technologie blockchain poměrně úzce souvisí s anonymitou transakcí. Blockchain coby účetní kniha ukládá do své databáze veškeré transakce, co byly provedeny, je to jeden z důvodů proč kryptoměny mohou fungovat bez centrální autority jako klasická fiat měna. Zároveň pro kryptoburzy tato technologie nabízí možnost v případě podezřelých transakcí je zmrazit a zkontrolovat, zda se nejedná

o formu trestné činnosti a v případě zjištění že ano předat příslušným orgánům Policie. Pro zločince může být blockchain zároveň nástrojem pro jejich aktivity, jak již bylo vyjádřeno v minulém bodě buď skrze série transakcí, jenž vytvoří tak spletitou síť, že zpětně je velice náročné se jimi propracovat pro vyšetřovatele anebo využíváním soukromých sítí, do kterých autority nemají přístup.

- Kryptoměny tím, že pracují v kyberprostoru na internetu mají vesměs okamžitý globální dosah. To znamená, že vývoj jejich hodnoty, se děje okamžitě pro všechny na světě a kdokoli s připojením k internetu je může používat jak pro legální, tak i nelegální činnosti.
- V návaznosti na předchozí bod může být vysvětlena i rychlost transakcí. V důsledku toho, že kryptoměny pracují v peer to peer síti, přes internet, bez centrální autority a v blockchainu se transakce dějí téměř okamžitě. To je rozdíl od klasického bankovního systému, který sice v dnešní době odesílá a provádí některé transakce velice rychle, zároveň banky transakce kontrolují a mohou je zastavit v případě nějaké anomálie která by poukazovala na nelegální činnost, to do určité míry provádějí i kryptoburzy, ale ne v takové míře jako banky, potažmo existuju spoustu možností převést kryptoměny bez té pomyslné třetí strany čímž možnost kontroly zaniká.
- Globálně platí, že kryptoburzy si za převody kryptoměn účtují nižší transakční poplatky než klasické finanční instituce jako třeba banky. To je třeba jeden z důvodu vzniku kryptoměny XRP, kdy byla jedna z prvotních myšlenek snaha zmenšit poplatky při mezinárodních převodech peněz.
- Šifrování kryptoměnových peněženek a plateb pracuje na principu 256 znaků jedniček a nul. Matematicky je sice možné tuto formu zabezpečení prolomit, ale fakticky prolomena nebyla. Teoretická šance na prolomení je přirovnatelná jako 9x v řadě vyhrát loterii. Opět se jedná o další silnou stránku, jenž je pro zločince taktéž přínosná, protože jimi držené peníze se nacházejí v peněžence, kde je šance vstupu neoprávněné osoby matematicky sice možná, ale velice nepravděpodobná.

6.1.2 Slabé stránky

- Vysoká volatilita může být pro investory někdy i kladná, hodnota se může měnit o výši desítek procent denně, mnohdy i mnohem více. Ovšem jako kryptoměny mohou na hodnotě získat, stejně mohou i ztratit, proto tuhle vlastnost autor obsáhl do slabin, protože pokud může určitá vlastnost být ku prospěchu a stejnou měrou i k neprospěchu tak je potřeba spíše uvažovat o tom negativním aspektu. Aktuální

příklad vývoje ceny 1 BTC, kdy byla hodnota dne 12.10.2023 26 750 USD a dne 12.02.2024 49 938 USD. Což znamená nárůst 23 188 USD za 4 měsíce. Dále si lze ukázat příklad ceny ze dne 12.11.2021 kdy hodnota 1 BTC byla 64 400 USD a o necelé 2 měsíce později čili dne 21.01.2022 byla hodnota 35 070 USD což je pokles o 29 330 USD.

- Omezená akceptace některých zemí může být způsobena z několika důvodu, mezi nejhlavnější lze řadit snahu státu mít kontrolu pro měnu své země a nedávat obyvatelům možnost alternativy. Země s úplným zákazem kryptoměn jsou např. Kamerun, Gabon, Lesotho. Pak existují země, které kryptoměny přímo nezakazují, ale snaží se je svými zákony regulovat. Do této role patřila Čína do roku 2021, ovšem aktuálně je BTC v Číně zakázán úplně. Rusko kryptoměny reguluje zákony, snaží se mít na nimi dohled, zároveň je spojuje s trestnou činností, ale úplně je nezakázalo. Nesmí je vlastnit státní zaměstnanci a dle ruských zákonů lze znárodnit takové kryptoměny, jenž pocházejí z trestné činnosti. Na druhé straně existují nepřímé důkazy, že zrovna na území Ruska se nacházejí servery s uzavřenými kryptoměnovými burzami a blockchainy, kde se provozuje právě nelegální činnosti, respektive transakce za tyto činnosti. Turecko v době své nejvyšší inflace vydalo nařízení, které zakazuje používání kryptoměn k platbám za zboží a služby, protože obyvatelé v důsledku inflace přecházely právě na kryptoměny. Pro zločince to může být taktéž poměrně komplikované, pokud chtějí svou činnosti provozovat na územ jednoho nebo více státu, kde jsou kryptoměny regulované nebo zakázané tak to znamená, že budou muset najít alternativu čímž nejspíše přijdou o výhody kryptoměn a vystaví se větší šanci k odhalení, což je ale samozřejmé pro veřejnost přínosné.
- Neregulovaný trh je poměrně široký pojem, do kterého se řadí spousty potenciálních problému, jež jsou důsledkem nedostatku regulace a dozoru ze strany vlád a finančních institucí. Pro investory mohou představovat komplikace právní a daňové nejistoty ohledně používání, držení a zdanění kryptoměn což může způsobit nepředvídatelné náklady pro jednotlivce nebo právnické osoby. Podstatně vyšší riziko nesou bezpečnostní problémy. Kvůli nedostatku regulace vznikají nezabezpečené kryptoměnové platformy, burzy a blockchainy, kde mohou být poctiví investoři napadeni a mohou být připraveny o své aktiva, zároveň se tyto platformy využívají hojně při nelegálním činnosti. V teoretické části autor zanalyzoval kryptoměnové podvody, jenž se aktuálně v kyberprostoru dějí. Tyto podvody mají širokou základnu, jak je lze provádět a neustále se vyvíjejí

a jsou sofistikovanější. Mezi nejčastější patří podvodné kryptoměny, kde autor zmizí se získanými prostředky a za sebou nechá bezcennou kryptoměny, formy phisningu, legalizace výnosů z trestné činnosti, vydírání, nákup za zboží a služby na černých tržištích a částečné financování terorismu.

- Energetická náročnost těžby kryptoměn a provozu jejich síti je dalším poměrně velkým problémem. Společnost aktuálně klade důraz na spotřebu elektrické energie, její výrobu a obnovitelnost. Těžba BTC je aktuálně zisková i přes velkou náročnost, ovšem z pohledu ekologie může být na ní nahlíženo, zda je ekonomický prospěch opodstatněn vůči udržitelnosti planety. Univerzitní badatelé uvedli, že jenom samotný Bitcoin, jeho těžba a provoz sítě ročně spotřebuje kolem 121 terawatthodiny. Pro představu jaderná elektrárna Temelín a Dukovany vyrobili za rok 2023 30.4 terawatthodiny. Spotřeba 121 terawatthodiny je stejná jako roční spotřeba celé Argentiny a vyšší než třeba Nizozemska, Norska a zhruba dvojnásobně vyšší než celé české republiky.

6.1.3 Příležitosti

- Technologický pokrok je aktuálním fenoménem, technologie napříč různými segmenty se vyvíjejí velikou rychlostí, zdokonalují se a reagují na aktuální trendy a požadavky společnosti což je také případ kryptoměn. U nich je kladen důraz na bezpečnost, a i přes fakt že je lze využívat k nelegálním činnostem, samotné kryptoměnové burzy se snaží tato jednání odhalovat a potírat je. Kryptoměny a jejich provozovatelé se snaží zlepšovat aspekty, kde klasická fiat měna zaostává tím, že dělá své služby dostupnější, transparentní, rychlé apod.
- Narůst uživatelů kryptoměn je způsobem mnohými faktory, jedním z předních je také to, že kryptoměny přijímají různé instituce a tím se jejich používání v očích mnoha lidí stereotypuje, je to dáno také tím, že existují již nějaký čas, jsou relevantní a mnozí investoři s nimi obchodují pro získání zisku, jiní uživatelé je používají pro jejich silné stránky jako je třeba určitá anonymita transakcí, rychlost apod.
- Digitalizace měny je pojem, který v dnešní společnosti již nějakou dobu je. Klasické bankovky a mince tvoří zhruba 5 % peněz v oběhu, zbytek je uložen pouze digitálně na bankovních účtech a platí se jimi elektronicky, což znamená, že kdyby se lidé pokusili v jeden moment vybrat veškeré své elektronické peníze, tak to nepůjde, protože fyzicky neexistují. EU v roce 2021 spustilo projekt digitální euro, myšlenka se opírá o to, že by každý občan eurozóny měl svou

virtuální peněženku s eury, kterými by mělo jít platit v rámci eurozóny a byl by pod záštitou evropské banky. Příležitostí by ale mohlo být pro tyto účely začít využívat kryptoměny jako je Bitcoin, které již existují a jsou prověřeny časem.

6.1.4 Hrozby

- Regulační hrozby by mohly mít za následek změny, které by hlavní důvody proč používat kryptoměny, oslabili. Pokud by státní instituce začali kryptoměny regulovat stejně jako klasickou měnu, přišly by o svou decentralizovanost a to by mohlo uživatele odradit od jejich používání, vesměs by mohli ztratit motivaci je používat, protože by se již nemuseli dostatečné odlišovat od konvenčních peněz.
- Negativní mínění veřejnosti je dalším podstatnou hrozbou pro kryptoměny, lze na to nahlížet z dvou hlavních pohledů a sice že určitá skupina lidí takovéhle platidlo nepřijímá, protože v něj nevěří, mohou to považovat jako podvod, technologii, jež využívá důvěřivost jiných a brzy skončí apod. Další skupina lidí může na kryptoměny pohlížet jako platidlo které vzniklo hlavně pro účely nelegálních činností a nenahlížejí na ně z roviny legálního platidla. Pokud většina veřejnosti převezme tyto negativní postoje, může to ohrozit samotnou existenci kryptoměn, kde není zákazník není ani zisk a bezcenná kryptoměna nemusí existovat. Navíc pokud by veřejnost vyžadovala zvýšenou regulaci tak lze předpokládat, že státy takovým požadavkům mohou začít vyhovovat.
- Umělá inteligence je aktuálně jedna z podrobně sledovaných technologií, od možností ji pokládat otázky na které odpovídá vcelku mnohdy jako lidská bytost, po generování fotografií, jež jsou k nerozeznání od skutečných fotek po aktuální možnost generování videí, které jsou také k nerozeznání od skutečného videa. AI Sora je zatím nedostupná veřejnosti, ale existuje předpoklad, že vzniknou podobné programy, jež zvládnou generovat obdobně věrná videa. Podvodníci již používají různé druhy nátlaku, vydírání apod pro získání zisku i přes kryptoměny, ale podvodníci zatím nemají k dispozici takto sofistikovaný nástroj. Kdyby jej získali, tak mohou vygenerovat téměř cokoliv. Pro člověka, jež má veřejné sociální sítě vzniká nebezpečí, že bude vygenerován on sám při nějaké činnosti a následně bude vydírán apod.

6.2 Strukturovaný rozhovor

Autor pro účely vypracování strukturovaného rozhovoru oslovil vrchního komisaře Policie ČR pana nadpraporčíka Bc. et BC. Erika Navrátila jenž působí v řadách policie jako odborník na vyšetřování trestných činů spojených s využíváním kryptoměn.

1. **Jaký je aktuální stav využívání kryptoměn jako platebního prostředku při nelegálním obchodu v ČR?**

„Kryptoměny jsou neregulovatelnými platebními prostředky, které se chovají jako akcie. Jejich hodnota velmi rychle kolísá. V současné době se používají jako legální platební prostředek. Lze je směnit za téměř jakoukoli měnu na světě i za jiné kryptoměny. Často se používají při spekulacích, a mnoho lidí se tak snaží vydělat rychlé peníze. Bohužel, tím, že jsou neregulované a nikdo nad nimi nemá centrální dohled, používají se také při trestné činnosti, a to velmi výrazným způsobem. Veškeré odcizené peněžní prostředky z bankovních účtů obětí, například při Vishingu nebo Phishingu, ale také při podvodech typu Romance Fraud nebo reverzních inzertních podvodech, končí na různých kryptoměnových účtech (peněženkách). Pachatelé využívají tento způsob, neboť získání kryptoměny na jednom místě na světě nebrání tomu, aby v rámci vteřin byla užita na opačné straně planety. Odcizené peněžní prostředky jsou jako zprostředkovaný výnos přeměněny na kryptoměnu, a tu už zpravidla nikdo nedohledá. Různé burzy působící ve virtuálním světě mají sídla v různých zemích světa, a v každé z těchto zemí platí jiné zákony. Vyžádat informace o různých kryptoúčtech je velmi složité a často nemožné. Některé burzy jsou si vědomy takto páchaných skutků, ale protože z každé transakce mají provizi, zavírají před těmito podvody oči. Spolupráci poté odmítají s odkazem na ochranu klientova soukromí. Trasování výnosů a nástrojů z trestné činnosti (v tomto případě peněz) vede pouze do pár kryptoúčtů, neboť narazíme-li na kryptoúčet s jedním vstupem, ale mnoha výstupy, nevíme, kam výnos (peníze) nakonec odešly, a trasování je tak u konce. A protože u mnoha kryptopeněženek platí, kdo ji vlastní a vlastní heslo, je majitelem, majitelé se tak v průběhu času mohou měnit. Je zde tedy mnoho proměnných a v dnešní době je kryptoměna způsob, jak „zlegalizovat" kradené virtuální peníze."

2. **Jaké konkrétní příklady nelegálních aktivit spojených s kryptoměnami jste během své kariéry zaznamenal?**

„Těch případů je velmi mnoho. Dá se říci, že téměř každý sofistikovaný případ páchaný organizovanou zločineckou skupinou (klasická callcentra – volač, klikař, bankéř…) vede nakonec do kryptoměn. Je to způsob, jakým pachatelé ukrývají svůj výnos, tedy ukradené peněžní prostředky, respektive peněžní prostředky ve formě jedniček a nul.

První a klasický případ je Vishing. Zavolá zaměstnanec banky, policie nebo bezpečností technik banky a volajícímu uvede, že byl jeho bankovní účet napaden. Vyvíjí nátlak a žádá o rychlé přeposlání všech peněz na bankovním účtu oběti na předem nadefinované bankovní účty třeba i u jiných bank. Oběť zahlcena informacemi a spěchem se přihlásí do internetového bankovnictví a veškeré své peníze pošle na tyto nadiktované účty. Jsou to účty české, zpravidla jiné oběti, kdy v reálném čase takto okrádají více lidí. Takto převedou peníze několikrát mezi české bankovní účty a poté všechny míří do kryptoměn na různé burzy, zpravidla Binance, Moonpay, Coinbase, Bybit…

Dalším případem jsou různé reklamy na investování nacházející se na instagramu, facebooku, nebo různých internetových stránkách. Všechny odkazují na různé druhy investic a zisků. Užívají přitom obrázky prezidenta republiky, známých osobností, společnosti ČEZ a podobně. Různým způsobem pak pachatelé oběť přesvědčí, ať si založí kryptoúčet zpravidla na jejich phishingových stránkách. Na tyto falešné účty oběti zasílají peníze a pachatelé si je samozřejmě ukládají v kryptoměnách na své účty.

Fraud Romance – Romantické podvody. Pachatel se vydává za někoho jiného na zřízeném falešném profilu, např. na facebooku. Vyhledává spíše postarší a osamělé osoby, muže či ženy a nabízí jim vztah. V určité fázi důvěry pak požádá o půjčku nebo zaslání peněz s jinou záminkou. Oběti pak důvěřují a peníze zasílají. I zde jsou využívány kryptoúčty a převoz peněz na kryptoměnu.

Kryptoměna se hojně užívá i u sofistikovaných reverzních inzertních podvodů. Prodávající nabízí zboží a kupující (pachatel) ho přiměje, aby vložil informace o své platební kartě či internetovým bankovnictví do phishingových internetových stránek, které vypadají jako platební brána dopravce např. DPD či České pošty. I zde nakonec odcizené peněžní prostředky končí zpravidla velmi rychle na kryptoúčtu. Nedají se podle českých zákonů zajistit jako výnos (to lze jen na tuzemských bankovních účtech).“

3. **Jaké jsou hlavní výzvy a obtíže, kterým čelíte při detekci a vyšetřování těchto případů?**

„Hlavní obtíž je, že nelze kryptoměny reálně trasovat, nelze je rychle zajistit a nelze ani zjistit skutečného majitele kryptoúčtu, na který byla tato kryptoměna zaslána. V reálu to znamená, že takto získané a přeměněné peněžní prostředky na kryptoměnu pachatelé každých pár minut převedou z jedné kryptopeněženky do druhé a zase dál a dál a během jednoho dne takto provedou i desítky, někdy i stovky převodů. Je to z důvodu, že se může stát, že by dotyčná burza spolupracovala s Interpolem nebo Europolem

a kryptoúčet by blokla resp. užila Freezing (zmražení účtu i kryptoměny). Proto se takto nelegálně získaná kryptoměna rychle přesouvá sem a tam, až nakonec skončí v neustanoveném clusteru. Prostě je nedohledatelná.

Za výzvu mohu považovat jakoukoli další možnost se na tomto úseku vzdělávat a praxi tak posouvat blíže k odhalení pachatelů. Avšak veškeré burzy a nebankovní instituce, které se kryptoměnami zabývají, jsou tzv. nikdezdejší a všudezdejší, takže působí na celém světě a v celém internetovém prostoru. Proto bude výzvou spíše sjednotit postupy v rámci mezinárodních organizací a mezinárodního práva, aby bylo reálné i v České republice dohledávat pachatele působícího například v Gruzii."

4. **Jak spolupracujete s dalšími orgány a mezinárodní institucemi při vyšetřování případů týkajících se kryptoměn a nelegálního obchodu?**

„Existují tři způsoby, jak s mezinárodními institucemi, organizacemi nebo orgány spolupracovat. První způsob je oslovit je napřímo. Někteří z nich mají pro tyto účely zřízeny zvláštní e-maily nebo internetové stránky, do kterých lze vložit různé požadavky policejního orgánu. Leckdy je nutná registrace, aby si ověřili, že jim píše skutečný policista. Zpravidla tato žádost musí být přeložena do anglického jazyka. Někteří z nich ještě požadují odkaz na zákon a paragraf v České republice, aby si ověřili, zda něco podobného mají i v zemi, ve které sídlí. Výsledek je pak různý a trvá různě dlouhou. Samozřejmě je to na bázi dobrovolnosti dané instituce nebo organizace. Výsledek také nelze užít jako důkaz.

Druhý způsob je využít nějaký z Českých zdrojů mezinárodní spolupráce. Resp. policejních zdrojů. Jedná se o organizaci v rámci policie, kterou je Ředitelství mezinárodní policejní spolupráce, ARO, CARIN nebo využití služeb vztyčného důstojníka v zemi, do které chceme žádost zaslat. Zase v tomto případě záleží na zemi, kam chceme žádost poslat. Vztyční důstojníci jsou pouze v některých zemích poblíž České republiky. ARO působí v rámci Schengenu, CARIN pak v rámci několika světadílů. Odpovědi ale nemusí vůbec dorazit, a pokud dorazí, tak se nedají užít jako důkaz.

Třetí způsob je využít zákon o Mezinárodní justiční spolupráci. Jediný způsob, jak získanou odpověď užít jako důkaz, který obstojí i před soudem. Avšak, záleží na státě, zda tento zákon ratifikoval a záleží na konkrétním státě a na jeho kultuře a úrovni justice. Z Německa přijde odpověď určitě a relativně brzy, kdežto například z Jihoafrické republiky, Číny nebo Vietnamu možná i takovýmto způsobem nedorazí.

Jiný způsob, jak komunikovat s institucemi, organizacemi a orgány mimo českou republiku není. Například Somálsko neodpoví nikdy, ani asi neví, že nějaká kyberkriminalita existuje.“

5. **Jaká opatření a legislativní změny a regulace kryptoměn by podle vás mohly pomoci v boji proti nelegálnímu využívání kryptoměn?**

„Zde platí asi dvě možnosti. Buď kryptoměny napříč celým světem v rámci legálnosti zakázat a tím je odkázat na jejich zánik, nebo je začít regulovat a centralizovat a stejně tak regulovat účty, na kterých se ukládají. To je však asi v rozporu se smyslem kryptoměny. Takže jsem přesvědčen, že pokud nějaký stát začne kryptoměny regulovat aspoň z části, aby se tak zamezilo jejich užívání pro nelegální transakce, jiný stát to neudělá a podvodníci se tak prostě přesunou do jiného státu, který jim dává více volnosti. Navíc, v současné době existuje přes 10.000 kryptoměn a nespočet burz, které neustále vznikají a zanikají a některé z nich nejsou pod žádným dohledem. Myslím si, že je nemožné legislativně podchytit nelegální využívání kryptoměn. Dokud budou existovat, budou užívány k nelegální činnosti. Analogicky, pokud bude existovat člověk, bude se stále krást (myšleno drobné krádeže, vloupání do vozidel, sklepů apod.).“

6. **Jaké kriminologická specifika byste zmínil ve spojitosti s využíváním kryptoměn?**

„Určitě anonymitu. Vlastníci kryptoměny, kteří nechtějí být známy, zůstanou v anonymitě a systém je nastaven tak, že i můžou. Dostupnost, globálnost. Na rozdíl od normální měny, která platí pouze v daném státě (výjimkou např. EURa) je kryptoměna schopna být uplatněna téměř kdekoli na světě, a to poměrně za velmi krátkou dobu. Latence, tím, že neexistuje centralizace a regulovatelnost, je kryptoměna „skryta“ před úřady a příslušnými orgány.

Kryptoměny jsou jako výnos z trestné činnosti téměř nedohledatelné, a to je problém, na který nestačí žádný stát samostatně.“

7. **Považujete počet policistů, kteří vyšetřují tyto trestné činy za dostatečný? Považujete zároveň jejich úroveň odbornosti za dostatečnou?**

„Obecně je policistů velmi málo. Pokud budu hovořit o současných tabulkových místech, tak ty rozhodně naplněny nejsou. Může reálně chybět tak 2.000 policistů. A pokud by tito policisté nechyběli, i tak je jich málo, neboť s příchodem Ukrajinců žádající o azyl chybí policisté do řad cizinecké policie, neustále se zvyšuje počet vozidel na pozemních komunikacích, takže chybí příslušníci dopravní policie a staví se nové

rodinné domy, takže plochy zastavených částí obcí a měst se rozšiřují, což je pak náročné na hlídkovou službu. Takže policisté chybí, a to jsem nezmínil, že dle statistik tvoří kyberkriminalita 10 procent majetkových trestných činů. Reálně je to tak 25 procent. Spousty lidí, se kterými se v praxi setkám a kteří vystupují jako „bílý koně" sami přijdou podvodem o peníze, ale nahlásit to nejdou. Takovýchto lidí je daleko víc než těch, kteří to nahlásí. Proto si myslím, že kyberkriminalita za 5 až 10 let dosáhne značných rozměrů. A jelikož chybí běžní policisté do ulic, je jasné, že policisté vyšetřující kyberkriminalitu nejsou skoro vůbec. Tvoří je obyčejní policisté, kteří nemají IT vzdělání, žádné kurzy a zdokonalují se pouze praxí a samostudiem. Při náboru k policii ČR postačí maturita, to mluví samo za sebe. Kyberkriminalita, extremismus apod. jsou specializace, které policista získá spíše samostudiem a praxí než vzděláním."

8. **Existují od policie určité formy školení/vzdělávání policistů pro vyšetřování těchto TČ?**

„Já osobně žádné takové nemám, a kdybych se o nějakém dozvěděl, tak bych se určitě přihlásil. Ale co sleduji, tak jsou spíše jednodenní přednášky specialistů, kteří pohovoří o praxi a o zjištěních získaných od kolegů z jiných zemí. Často to bývají soudní znalci v oboru IT, kteří přednášejí o své práci, která je spojena i s prací policejní."

9. **Znáte Moskevskou kryptoburzu Garantex? Pokud ano, jak byste mohl popsat činnost této burzy? Případně zaznamenal jste kryptoburzu s uzavřeným blockchainem, kde je podezření, že slouží zejména k trestné činnosti?**

„Bohužel tuto kryptoburzu neznám. Zpravidla jsou při páchání kyberpodvodů využívány burzy, prostřednictvím kterých je pak kryptoměna zasílaná dále. Burzy jsou zpravidla regulované a mají vysoké bezpečností prvky. Jde pak o účty, které jsou zde založeny na totožnost obětí nebo neexistujících lidí. Reálně, sídla organizovaných skupin byla odhalena pomalu po celém světě. Záleží tedy na tom, jakou burzu nebo kryptoúčty používají. Troufnu si tvrdit, že se policie dozví jen zlomek toho, kam vlastně kryptoměna putuje a je docela možné, že mnohá mohla skončit i na kryptoburze Garantex."

10. **Jak byste celkově shrnul možnosti policie při vyšetřování kryptoměn při nelegální činnosti?**

„Aby se mohlo vyšetřovat, je nutné opatřit důkazy a ty se zpravidla nejprve shání operativně. V tomto případě by operativa zasahovala do mnoha zemí, a to si troufnu říci, je nereálné. Takže možnosti má v tomto případě asi jen NCTEKK (Národní centrála proti terorismu, extremismu a kybernetické kriminalitě), který má i finanční prostředky

a kontakty na kolegy z jiných zemí. Já na úrovni okresní kriminálky moc nezmůžu. Navíc jsou kryptoměny pachateli užívány právě proto, že je policie víceméně na jejich zajištění a dohledání krátká.“

11. **Jaké jsou vaše doporučení pro jednotlivce a firmy, aby minimalizovaly rizika spojená s nelegálním využíváním kryptoměn?**

„Pokud se jedná o držení kryptoměny a její užívání jako měny, tak je nutné využívat služeb registrovaných burz, které jsou v zemi, kde mají sídlo, regulované a například i pojištěné proti úpadku. To se dá zjistit na internetu při troše hledání. Pokud se jedná o investice, tak užívat burzy s historií a též si ověřit, zda nad nimi dohlíží nějaký státní orgán. V dnešní době není těžké najít spousty recenzí a návodů na kryptoměny, kam investovat, co použít a jak bez rizika platit. Je tedy nutná a nezbytná obezřetnost a opatrnost.“

Závěr

V teoretické části bakalářské práce se autor soustředil na vysvětlení pojmu kryptoměna, výčtu základních pojmů souvisejících, popsání vzniku kryptoměn a následně přidáváním dalších nezbytných pojmů pro účely této práce jako je kyberprostor, kyberkriminalita a kybernetická bezpečnost. Pro vyhodnocení cílů bylo důležité popsat princip na kterém kryptoměny fungují, vysvětlit, jak funguje anonymita, jak fungují kryptoměnové peněženky, technologii blockchain apod.

Hlavním cílem práce bylo analyzovat využití kryptoměn jako platebního prostředku v nelegálním obchodě a zhodnotit možnosti na jejich právní regulaci. Analýza využití kryptoměn při nelegálním obchodě proběhla částečné již v teoretické části a v kombinaci se strukturovaným rozhovorem a SWOT maticí autor zjistil, že variabilita využití je široká z mnoha důvodů.

Kryptoměny se tedy využívají při nepřeberném množství různých podvodů, phishingů, vishingů. Je to aktuálně veliký problém, zločinci vymýšlejí stále nové a nové způsoby, jak podvody provádět, využívají k tomu sociální inženýrství, umělou inteligenci a své zkušenosti a každý den svými skutky způsobují velké škody. Zároveň svojí činností mohou dostat nevinné občany do situace kdy nevědomě páchají TČ z pozice legalizátora prostředků získaných TČ. Tím výčet využití kryptoměn při nelegální činnosti zdaleka nekončí, dále je lze využít jako platební prostředek na darknetu za různé zboží a služby jako jsou falešné identity, drogy a jiné zakázané položky, při vydírání je zločinci mohou využít jako formu pro platbu, v neposlední řadě je lze využít k financování terorismu a jiných extremistických skupin.

Možnosti jejich právní regulace je složité téma zejména s ohledem, že se jedná o celosvětový problém. Z teoretické části práce vyplývá, že zákony v ČR na tuto problematiku pamatují, to samé lze tvrdit i o EU, ale ze strukturovaného rozhovoru je na druhou stranu patrné, že stěžejním problémem je fakt, že spousta zemí po celém světě má buď zákony odlišné, nebo další země nejsou tak vyspělé, aby tuto problematiku nějakým způsobem potírali. Dle strukturovaného rozhovoru vyplývá, že pro budoucí právní regulaci by se musel postupně sjednotit právní systém všech zemí na světě v otázce kryptoměn, přičemž by musela být i na vysoké úrovni mezinárodní spolupráce anebo by mohlo být řešením kryptoměny úplně zakázat, případně nad nimi zřídit centrální autoritu. Aktuálně jsou obě metody nedosažitelné. Na území EU probíhá mezinárodní spolupráce dobře, policejní orgány komunikují a poskytují si potřebné informace, problémem ale je

fakt, že značnou část z těchto informací policie nemůže použít jako důkazní prostředek. To otevírá možnost diskuze na téma, jak vylepšit právní systém ohledně kryptoměn v EU. Ovšem po odstranění těchto právních nedostatků opět vyvstane překážka v podobě anonymity, kdy je pro policii téměř nemožné vystopovat platbu, která proběhla například mixérem.

Dílčím cílem bylo vyhodnotit a definovat kriminologická specifika kryptoměn jako platební prostředku. Mezi ty nejdůležitější patří možnost užívat kryptoměny anonymně, sice anonymita není úplná, jak je uvedeno v odborných zdrojích, ale ze strukturovaného rozhovoru vyplynulo že, pokud daná osoba ví, co dělá, tak je pro policii téměř nemožné takové platby vystopovat, zejména při využití nástrojů jako jsou mixéry. Globální dosah zase stěžuje spolupráci mezi jurisdikcemi při vyšetřování TČ. Absence státních institucí či centrálních bank znamená, že kryptoměny mohou být využívány bez kontroly a dohledu. Pomocí kryptoměn jsou financovány nelegální aktivity, což kriminalistům stěžuje nejen odhalení plateb ale samotných zločinců, jenž v souběhu mohou konat vícero trestných činů např. dealeři drog, padělatelé apod. V rozhovoru dále byla zmíněna latentnost kdy zajištění důkazů a vyšetřování trestné činnosti prováděné s využitím kryptoměn může být obtížné kvůli nedostatečné transparentnosti této technologie a stopy zanechané v kyberprostoru anebo rovnou tím, že se o ní kriminalisté nedozvědí.

Dle autora by měly jednotlivé země vynaložit více pozornosti k této problematice a pokusit se najít kompromis k bezpečné existenci kryptoměn. Autor zastává názor, že úplný zákaz by sice zločincům zkomplikoval jejich činnost, ale nějakým způsobem by našly nové metody, jak pokračovat. Obrovský problém vidí v aktuálních podvodech, co se ukazují formou placené reklamy na sociálních sítích a celkově v prostředí internetu. Setkal se několikrát s tím, že mu byla spuštěna reklama na kybernetický podvod a považuje tyto reklamy za dobře zpracované, několikrát byl sám na portálech s bazarovým zbožím apod. osloven kybernetickými podvodníky. Tito lidé využívají různé metody psychických nátlaků a sociálního inženýrství a pro důvěřivé osoby které mají úroveň znalosti počítače pouze na slabší uživatelské úrovni může být velice obtížné rozeznat, zda se jedná o podvod či nikoliv. Navíc technologie umělé inteligence se vyvíjí rychle a je otázkou kdy budou podvodníci schopni dělat nerozeznatelné reklamy od těch pravých.

Výzkum byl pro autora velmi přínosný, sám o téhle problematice zpočátku věděl pouze základy, neznal, jak kryptoměny fungují a jakým způsobem zločinci mohou kryptoměny využívat. Tato práce mu poskytla spoustu důležitých informací a osvětlila

mu tuto problematiku. Během dokončování měl autor možnost poradit člověku, který se mohl stát obětí kybernetického podvodu pouze na základě znalostí načerpaných během tvorby této práce, což bylo pro danou osobu velice přínosné a pravděpodobně jí to pomohlo od škody.

Seznam použitých zdrojů

Literární zdroje

1. ANTONOPOULOS, A. M. *Mastering bitcoin.* Sebastopol CA: O´Reilly, 2015. 368 s. ISBN 978-1-449-37404-4.
2. GŘIVNA, T. et. al. *Kriminologie, 4. rozšířené vydání.* Praha: Wolters Kluwer. 2014. 530 s. ISBN: 978-80-7478-614-3.
3. KALISKÝ, B. *Bitcoin a ti druzí: nepostradatelný průvodce světem kryptoměn.* Praha: IFP Publishing s.r.o., 2018. 136 s. ISBN 978-80-87383-71-1.
4. KOHOUT, R. *Bezpečnost v online prostředí.* Karlovy Vary: Biblio Karlovy Vary, 2016. 64 s. ISBN978-80-260-9543-9.
5. KOLOUCH, J. *CyberCrime*, 1. Edice CZ.NIC. Praha, 2016, 526 s. ISBN 978-80-88168-34-8.
6. KOLOUCH, J. et. al. *Cybersecurity.* Praha. Edice CZ.NIC. 2019. 560 s. ISBN 978-80-88168-31-7.
7. KOLOUCH, J. et. al. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha. Policejní akademie České republiky v Praze, 2013. 117 s. ISBN 978-80-7251-402-1.
8. KRISTKO, O. CH. et. al. *Krypto jednoduše: nejen o bitcoinu pro začátečníky.* Praha: Fisio/Cuddle, 2023. 176 s. ISBN 978-80-908809-0-0.
9. KULHÁNEK, P. *XRP, vládce kryptoměn, aneb bitcoin nemá důvod k existenci.* Litomyšl: H.R.G. spol. s.r.o., 2020. 187 s. ISBN 978-80-88320-28-9.
10. LÁNSKÝ, J. *Kryptoměny.* Praha: C.H. Beck, 2018. 144 s. ISBN 978-80-7400-722-4.
11. LEWIS, A. *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them.* Coral Gables: Mango publishing 2021. 408 s. ISBN 978-1-6425-673-0.
12. POLČÁK, R. et. al. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. 656 s. ISBN 978-80-7598-045-8.
13. POPPER, D. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to neinvent money.* New York: HarperCollins Publishers, 2015. 432 s. ISBN 978-0-06-236249-0.
14. POŽÁR, J. et. al. *Kybernetická bezpečnost, hospodářská kriminalita a bezpečnostní management ve vzájemných souvislostech.* Praha. Policejní akademie ČR. 2020. 328 s. ISBN 978-80-7251-505-9.

15. PRITZKER, Y. *Vynález jménem bitcoin.* Přeložil Tereza WONGOVÁ. Praha: Braiins Publishing, 2020. 112 s. ISBN 978-80-907975-0-5.
16. SEDLÁK, P. et. al. *Kybernetická (ne)bezpečnost.* Brno. Akademické nakladatelství CERM. 2021. 440 s. ISBN 978-80-7623-068-2.
17. STROUKAL, D. et al. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání.* Praha: Grada Publishing 2021. 294 s. ISBN 978-80-271-1043-8.
18. TOMÁŠEK, J. *Úvod do kriminologie.* Plzeň: Aleš Čeněk s.r.o. 2019. 215 s. ISBN: 978-80-7380-746-7.
19. VÁLKOVÁ, H. et al. *Základy kriminologie a trestní politiky, 3 vydání.* Praha: C.H.Beck. 2019. 616 s. ISBN: 978-80-7400-732-3.
20. ZAPLETAL, J. et al. *Kriminologie, 3. vydání.* Praha: Wolters Kluwer. 2008. 528 s. ISBN: 978-80-7357-377-5.

Elektronické zdroje

1. *5 důvodů, proč aktualizovat software.* [online] 26.09.2019 Evropská unie. [cit. 2024-02-07] Dostupné z WWW: https://portaldigi.cz/5-duvodu-proc-aktualizovat-software/
2. ALI, S. *Peníze přes kryptoměny vyprat lze, záznam ale zůstane navždy, říká expert.* [online] 15.01.2023. iDnes. [cit. 2024-01-30] Dostupné z WWW: https://www.idnes.cz/ekonomika/zahranicni/binance-jarek-jakubcek-kryptomeny-prani-spinavych-penez.A230108_123335_eko-zahranicni_alis
3. BARTOK, J. *Co jsou to kryptoměny? Vítejte ve světe digitálních peněz.* [online]. 13.04.2022. Portu magazín. [cit. 2023-10-30] Dostupné z WWW: https://magazin.portu.cz/co-jsou-to-kryptomeny-vitejte-ve-svete-digitalnich-penez/
4. *Co je ARPANET.* [online]. Správa sítě. [cit. 2023-10-31] Dostupné z WWW: https://www.sprava-site.eu/arpanet/
5. *Co je brána Firewall?* [online] Microsoft. [cit. 2024-02-07] Dostupné z WWW: https://support.microsoft.com/cs-cz/office/co-je-br%C3%A1na-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603
6. *Co je kybernetický útok.* [online] 13.09.2022. Legislativa. [cit. 2024-02-08] Dostupné z WWW: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

7. *Co je to antimalware a firewall a proč je používat?* [online] 14.02.2017. Vim kam klikam. [cit. 2024-02-07] Dostupné z WWW: https://www.vimkamklikam.cz/rady-a-tipy/co-je-to-antimalware-a-firewall-a-proc-je-pouzivat
8. *Co je trojský kůň.* [online] Správa sítě. [cit. 2024-02-09] Dostupné z WWW: https://www.sprava-site.eu/trojsky-kun/
9. ČIHÁK, L. *Co je to Dark Web, jak se na něj dostat a kam se na něm vydat?* [online] 29.11.2022 CDR [cit. 2023-11-27] Dostupné z WWW: https://cdr.cz/clanek/co-je-dark-web-jak-se-na-nej-dostat-kam-se-na-nem-vydat
10. *Dark web a deep web aneb temná zákoutí internetu.* [online] 15.5.2023 Krytoland [cit. 2023-11-27] Dostupné z WWW: https://www.krytoland.cz/dark-web-a-deep-web-aneb-temna-zakouti-internetu
11. *Definice pojmu terorismus.* [online] 29.07.2009. MVCR. [cit. 2024-01-31] Dostupné z WWW: https://www.mvcr.cz/clanek/definice-pojmu-terorismus.aspx
12. DEYL, D. *Kryptoburza, íránci i západ: kde bere hamás peníze?* [online] 01.11.2023. Týdeník hrot. [cit. 2024-01-31] Dostupné z WWW: https://www.tydenikhrot.cz/clanek/kryptoburza-iranci-i-zapad-jak-se-financuje-hamas
13. DLUBALOVÁ, K. *Na nebezpečí kyberkriminality upozorní Den bezpečnější internetu.* [online] MVCR. [cit. 2024-01-17] Dostupné z WWW: https://www.mvcr.cz/clanek/na-nebezpeci-kyberkriminality-upozorni-den-bezpecnejsiho-internetu.aspx
14. FANTA, M. *Znáte nejčastější kryptoměnové podvody?* [online] Cyberblog. [cit. 2024-01-30] Dostupné z WWW: https://cyberblog.cz/crypto/znate-nejcastejsi-kryptomenove-podvody/?gad_source=1&gclid=CjwKCAjw17qvBhBrEiwA1rU9w23zJ80jxKDBKFc1iJtiVWcU69PPx_ft0jHDfZ1VQ1Bi70XGBG6zFRoCtNgQAvD_BwE
15. *Fenomén jménem kryptoměny – proč jsou tak populární?* [online] 30.01.2022. Měšec. [cit. 2024-03-11] Dostupné z WWW: https://www.mesec.cz/pr-clanky/fenomen-jmenem-kryptomeny-proc-jsou-tak-popularni/

16. FILIPOVÁ, K. *Česká republika po osmi letech ratifikovala Úmluvu o počítačové kriminalitě.* [online] 29.8.2013 Ekonom. [cit. 2023-12-12] Dostupné z WWW: https://pravniradce.ekonom.cz/c1-60516560-ceska-republika-po-osmi-letech-ratifikovala-umluvu-o-pocitacove-kriminalite
17. GREGOR, M. *Nejtypičtější krypto podvody: Na tyto věci si dávejte extra pozor!* [online] 19.02.2023. Kryptonovinky. [cit. 2024-01-30] Dostupné z WWW: https://www.kryptonovinky.cz/krypto-podvody/
18. HADRAVA, L. *Pradědečkem internetu je arpanet.* [online] ČT24. [cit. 2023-10-31] Dostupné z WWW: https://ct24.ceskatelevize.cz/svet/1387310-pradedeckem-internetu-je-arpanet
19. HOKROVÁ, V. *Legalizace výnosů z trestné činnosti z nedbalosti.* [online] 25.2.2022. Policie ČR. [cit. 2023-12-26] Dostupné z WWW: https://www.policie.cz/clanek/archiv-zpravodajstvi-zpravodajstvi-2022-legalizace-vynosu-z-trestne-cinnosti-z-nedbalosti.aspx
20. *Jak na internet* [online]. 2017 [cit. 2023-10-25]. Dostupné z WWW: https://www.jaknainternet.cz/page/1205/historie-internetu/
21. KALABIS, Z. *Vysvětlení pojmu „legalizace výnosů z trestné činnosti“* [online] 11.11.2015. Zlatá koruna. [cit. 2023-12-26] Dostupné z WWW: https://www.zlatakoruna.info/zpravy/vysvetleni-pojmu-%E2%80%9Elegalizace-vynosu-z-trestne-cinnosti%E2%80%9C
22. Ken Shirriff. In YouTube [online] 2023-10-19. Dostupné z WWW: <https://www.youtube.com/watch?v=y3dqhixzGVo&ab_channel=KenShirriff>. Kanál uživatele Ken Shirriff
23. *Kriminalita v ČR a EU – 2012-2022.* [online] Kurzy. [cit. 2024-02-02] Dostupné z WWW: https://www.kurzy.cz/zpravy/743260-kriminalita-v-cr-a-eu-20122022-pro-mezirocni-narust-registrovane-kriminality-v-roce-2022-mela/
24. *Kyberkriminalita.* [online] 01.05.2021. Krnov. [cit. 2023-11-28] Dostupné z WWW: https://www.krnov.cz/kyberkriminalita/d-37431
25. *Kyberkriminalita.* [online] Policie ČR. [cit. 2023-12-11] Dostupné z WWW: https://www.policie.cz/clanek/kyberkriminalita.aspx
26. MACHAČ, O. *Co je to ethereum?* [online] 1.5.2021. Fintree. [cit. 2023-10-30] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/ethereum/

27. MACHÁČ, O. *Satoshi Nakamoto a Bitcoin.* [online] 20.11.2022. Fintree. [cit. 2023-13-10] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/satoshi-nakamoto-a-bitcoin/
28. MORAVČÍK, O. *Vývoj registrované kriminality v roce 2022.* [online] Policie ČR. 13.01.2023. [cit. 2024-01-17] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx
29. MORAVČÍK, O. *Vývoj registrované kriminality v roce 2023.* [online] 12.01.2024. Policie ČR. [cit. 2024-02-02] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx
30. MORAVČÍK, O. *Vývoj registrované kriminality v roce 2023.* [online] Policie ČR. 12.01.2024. [cit. 2024-01-18] Dostupné z WWW: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx
31. *Nejčastější podvody s Bitcoinem*. [online] 09.01.2024. Finex. [cit. 2024-01-30] Dostupné z WWW: https://finex.cz/nejcastejsi-podvody-s-bitcoinem-na-toto-si-dejte-pozor/
32. *Největší hrozby a příležitosti dark webu.* [online] 24.10.2022 Digital Security Guide [cit. 2023-11-28] Dostupné z WWW: https://digitalsecurityguide.eset.com/cz/nejvetsi-hrozby-a-prilezitosti-dark-webu?utm_source=twitter&utm_medium=post&utm_content=dsg&utm_campaign=sc10#h2-2
33. OULEHLA, R. *Co je bitcoin? Vše stručně a přehledně v jednom článku!* [online].17.03.2021. Fintree. [cit. 2023-10-30] Dostupné z WWW: https://fintree.cz/zakladni-pojmy/co-je-bitcoin/
34. PETŘÍK, J. *Těžba – mining*. [online] Btctip, 2023. [cit. 2023-10-25] dostupné z WWW: https://www.btctip.cz/tezba-mining/
35. *Phishing.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/phishing/
36. PILICI, S. *Don't Fall for the Double Your Bitcoin Scam Stealing Crypto.* [online] 02.11.2023. Malwaretips. [cit. 2024-01-30] Dostupné z WWW: https://malwaretips.com/blogs/double-your-bitcoin-scam/
37. *Počítačová kriminalita.* [online] Můj právník. [cit. 2024-03-10] Dostupné z WWW: https://muj-pravnik.cz/pocitacova-kriminalita/

38. *Ripple (VŠE, CO CHCETE VĚDĚT).* [online] 04.03.2020. Alza. [cit. 2024-01-31] Dostupné z WWW: https://www.alza.cz/ripple-xrp#co-je-to
39. RZYMAN, T. *Co je botnet?* [online] 27.10.2017. IP Technik, [cit. 2024-02-09] Dostupné z WWW: https://iptechnik.cz/co-je-botnet/
40. SASSEN, G. *Co je to ten mining pool (těžařský pool) a proč vlastně existuje?* [online] 08.11.2017. Bitcoinblog. [cit. 2023-10-25] Dostupné z WWW: https://bitcoinblog.cz/co-je-to-ten-mining-pool-tezarsky-pool-a-proc-vlastne-existuje/
41. SMOLÍK, J. *Financování terorizmu.* [online] 2017. Vojenské rozhledy. [cit. 2024-01-31] Dostupné z WWW: https://www.vojenskerozhledy.cz/kategorie-clanku/bezpecnostni-prostredi/financovani-terorizmu
42. *Sociální inženýrství.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/
43. *Statistické přehledy kriminality za rok 2023.* [online] Policie ČR. [cit. 2024-02-02] Dostupné z WWW: https://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2023.aspx
44. *Stav, struktura a dynamika kriminality.* [online] FSPS MUNI. [cit, 2024-01-17] Dostupné z WWW: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/stav
45. *Stav, struktura a dynamika kriminality.* [online] FSPS MUNI. [cit. 2024-02-02] Dostupné z WWW: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/stav
46. STREAM, 29.07.2022 *Spojil drogy s Bitcoinem a vydělal miliony. Příběh Rosse Ulbrichta.* Stream video. [cit. 2023-11-28] Dostupné z: https://www.stream.cz/ekonomie-lidskou-reci/spojil-drogy-s-bitcoinem-a-vydelal-miliony-pribeh-rosse-ulbrichta-64365225
47. STROUKAL, D. et al. *Bitcoin a jiné kryptopeníze budoucnosti, 3. rozšířené vydání.* Praha: Grada Publishing 2021. 20-27 s. ISBN 978-80-271-1043-8.
48. S*truktura kyberkriminality 2020.* [online] Policie ČR. [cit. 2024-01-12] Dostupné z WWW: https://veda.polac.cz/wp-content/uploads/2022/04/Pocitacova-mravnostni-kriminalita-%E2%80%93-kybergrooming.pdf
49. ŠPITÁLSKÁ, P. *Žena naletěla podvodníkovi. Na falešné investice do kryptoměny si vzala půjčku.* [online] 18.03.2023. Deník. [cit. 2024-01-30] Dostupné z WWW: https://berounsky.denik.cz/zlociny-a-soudy/zena-

naletela-podvodnikovi-na-falesne-investice-do-kryptomeny-si-vzala-pujcku-20.html

50. *Trojský kůň.* [online] Eset. [cit. 2024-02-09] Dostupné z WWW: https://www.eset.com/cz/trojsky-kun/
51. *Utekli se 75 miliony. Kryptoměna squid těžící z popularity seriálu Hra na oliheň byla obrovský podvod.* [online] 11.02.2021. iRozhlas. [cit. 2024-01-30] Dostupné z WWW: https://www.irozhlas.cz/zpravy-svet/kryptomena-squid-hra-na-olihen-podvod-krypto-trh-kradez-75-milionu_2111021206_vis
52. VÁCLAVÍK, L. *Vetšina internetu je skrytá. Co jsou to deep a dark web?* [online] 8.10.2018 Cnews. [cit. 2023-11-27] Dostupné z WWW: https://www.cnews.cz/clanky/co-je-to-deep-invisible-hluboky-dark-temny-web/
53. VÁCLAVÍKOVÁ, J. *Co přineslo Snowdenovo odhalení: Šifrovaná komunikace i omezení moci tajných služeb* [online] 11.6.2023 Aktuálně [cit. 2023-11-28] Dostupné z WWW: https://zpravy.aktualne.cz/zahranici/co-prineslo-snowdenovo-odhaleni-pred-10-lety/r~ea4780ea06c611eea3c0ac1f6b220ee8/
54. VÁVRA, J. *Půlení bitcoinu má poslat cenu kryptoměny do nebes. Držitelé na halving čekají čtyři roky.* [online]. 14.04.2023. E15. [cit. 2023-10-20] Dostupné z WWW: https://www.e15.cz/bitcoin-halving-2024.
55. VOKŘÁL, J. *Zatímco bitcoin padal, ethereum rostlo. Čím se od něj liší?* [online] 30.4.2021. Seznam zprávy. [cit. 2023-10-30] Dostupné z WWW: https://www.seznamzpravy.cz/clanek/ethereum-152608
56. WAGNER, J. *Dark web – proč děti zajímá a co jim tam hrozí* [online] 15.11.2022 Pedagogicke info [cit. 2023-11-28] Dostupné z WWW: https://www.pedagogicke.info/2022/11/kybcast-dark-web-proc-deti-zajima-co.html
57. WOLF, K. *Kryptoměny ve službách teroru?* [online] 18.10.2023. Lupa. [cit. 2024-01-31] Dostupné z WWW: https://www.lupa.cz/clanky/kryptomeny-ve-sluzbach-teroru/
58. *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online] NGSS. [cit, 2023-12-11] Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16

59. *Zpráva o stavu kybernetické bezpečnosti za rok 2017.* [online] 30.5.2017 NUKIB. [cit. 2023-12-19] Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/

Legislativní dokumenty

1. ČESKÁ REPUBLIKA. Zákon č. 40 ze dne 8. ledna 2009 trestní zákoník. In Sbírka zákonů, České republika. 2009, částka 11, Dostupné z WWW: https://www.zakonyprolidi.cz/cs/2009-40

Seznam zkratek

- BTC - Bitcoin
- XRP - Ripple
- ARPA - Advanced Research Project Agency
- IT - Information Technology
- ICT - Information and Communication Technologies
- PC - Personal computer
- ČR - Česká republika
- EU - Evropská Unie
- AIDS - Acquired Immune Deficiency Syndrome
- NCTEKK - Národní centrála proti terorismu, extremismu a kybernetické kriminalitě
- TČ - Trestný čin

Seznam tabulek, grafů, vzorce a obrázku

Seznam příloh

Přílohy

Příloha A – Otázky ke strukturovanému rozhovoru

1. Jaký je aktuální stav využívání kryptoměn jako platebního prostředku při nelegálním obchodu v ČR?
2. Jaké konkrétní příklady nelegálních aktivit spojených s kryptoměnami jste během své kariéry zaznamenal?
3. Jaké jsou hlavní výzvy a obtíže, kterým čelíte při detekci a vyšetřování těchto případů?
4. Jak spolupracujete s dalšími orgány a mezinárodní institucemi při vyšetřování případů týkajících se kryptoměn a nelegálního obchodu?
5. Jaká opatření a legislativní změny a regulace kryptoměn by podle vás mohly pomoci v boji proti nelegálnímu využívání kryptoměn?
6. Jaké kriminologická specifika byste zmínil ve spojitosti s využíváním kryptoměn?
7. Považujete počet policistů, kteří vyšetřují tyto trestné činy za dostatečný? Považujete zároveň jejich úroveň odbornosti za dostatečnou?
8. Existují od policie určité formy školení/vzdělávání policistů pro vyšetřování těchto TČ?
9. Znáte Moskevskou kryptoburzu Garantex? Pokud ano, jak byste mohl popsat činnost této burzy? Případně zaznamenal jste kryptoburzu s uzavřeným blockchainem, kde je podezření, že slouží zejména k trestné činnosti.
10. Jak byste celkově shrnul možnosti policie při vyšetřování kryptoměn při nelegální činnosti?
11. Jaké jsou vaše doporučení pro jednotlivce a firmy, aby minimalizovaly rizika spojená s nelegálním využíváním kryptoměn?